VIRGINIA DEPARTMENT OF
SOCIAL SERVICES

INFORMATION SECURITY POLICY and PROGRAM GUIDE

Prepared By:
Information Security and Risk Management

Date Document Prepared:
September 2016

Publication Version Control

Publication Version Control: It is the user's responsibility to ensure they have the latest version of this publication. Questions should be directed to the Virginia Department of Social Services (VDSS) Chief Information Security Officer (CISO) within the Information Security and Risk Management (ISRM) Office. The VDSS CISO will issue an agency-wide Broadcast and post the revised publication version on the Services.Programs.Answers.Resources.Knowledge (SPARK) Intranet, and provide an email announcement to State/Local Security Officers as well as other parties the VDSS CISO considers being interested in the change.

This chart contains a history of this publication's revisions.

Version	Date	Comments
Original	July 15, 1992	
Revision 1	April 3, 2001	
Revision 2	November 18, 2003	
Revision 3	May 2007	
Revision 4	May 2008	
Revision 5	April 2012	
Revision 6	August 2012	Final reviews complete. Forward to the Commissioner for approval. Effective upon publication to SPARK.
Revision 7	September 4, 2012	Final changes and new Non-Paid Employee status added.
Revision 8	February 2014	Contractor language clarified. Includes links to updated IT Management and Telecommunications Policy and Procedures and the Proactive Monitoring Program. IRS Data, Password Management, Firewalls, Administrative Accounts, and Data Sharing sections added as well as Bring Your Own Device.
Revision 9	April 2014	Final reviews complete. Forward to the Commissioner for approval. Effective upon publication to SPARK.
Revision 10	September 30, 2014	Name change and new employees language clarified. ***FTI*** and fax included.
Revision 11	February 2016	Updated in concert with NIST Special Publication 800-53 Revision 4 (.pdf) and Cybersecurity Framework. Updated policy governance and management allowing the VDSS CISO to develop and publish separate policy documents as needed for specific NIST/IRS/CMS/FBI/SSA control requirements. Significant updates to Risk Management, Wireless Security, Administrator Accounts, Encryption, and Change Management sections. Personnel security section updated to allow new employee security setup before first day of work.
Revision 12	September 2016	Updated Code of Virginia hyperlinks.

Review Process: The VDSS CISO and staff of the ISRM Office contributed to the review of this publication. All comments were carefully evaluated, and individuals that provided comments were notified of the actions taken.

PREFACE

Subject

The ***VDSS Written Information Security Policy and Program Guide***

Effective Date: February 19, 2016

Authority

The policies described in this document are based on requirements found in the following codes, policies, regulations, laws, standards and guidelines:

CMS MARS-E 2.0

Code of Virginia Social Service Laws 63.2 (2002)

FBI CJIS 5.4 (.pdf)

HHS 45 CFR 303.21 and 45 CFR 303.105

IRS Publication 1075 (.pdf)

IRS Revenue Procedure Section 6103 (L)(7)(b), Disclosure of Information to Federal, State, and Local Agencies

ITRM Policies, Standards and Guidelines

NIST Special Publication 800-53r4 (.pdf)

Social Security Program Rules

Temporary Assistance for Needy Families TANF Manual 103.1 (1/20/97), Purpose of Safeguarding of Information and Scope of Regulations

USDA/FNS 7 CFR 72.1 (c), 27.1 (d), Disclosure of Information

VDSS/DCSE Manual, Chapter 2 (11/1/96), Confidentiality/Information Release

Applicable Executive Orders and Directives

ED-06, EO-8, EO-39

Purpose

To define the ***VDSS Information Security Program***.

Scope

This policy applies to:

All *Individuals* (VDSS employees, Local Department of Social Services [LDSS] employees, contractors, vendors, volunteers, student interns, work experience personnel and other persons and organizations) who have a need to use VDSS- related information or information processing systems;

All information and information processing systems associated with VDSS; and

All information and information processing systems associated with other organizations which VDSS uses, including but not limited to the Social Security Administration (SSA), the Virginia Department of Taxation (TAX), the Internal Revenue Service (IRS), the Department of Motor Vehicles (DMV), and the Virginia Employment Commission (VEC).

In accordance with the *Code of Virginia* § 2.2-603, § 2.2-2009, and § 2.2-2010 VDSS is responsible for complying with Commonwealth Information Technology Resource Management (ITRM) policies and standards and considering Commonwealth ITRM guidelines issued by the Commonwealth of Virginia (COV) Chief Information Officer (CIO). In addition: "The director of every department in the executive branch of state government shall report to the CIO as described in § 2.2-2005, all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information systems with the potential to cause major disruption to normal agency activities. Such reports shall be made to the CIO within 24 hours from when the department discovered or should have discovered their occurrence."

Table of Contents

1. *VDSS Information Security Policy and Program* Guide Statement

1.1 Background

The Virginia Department of Social Services (VDSS) relies heavily on the application of information technology for the effective delivery of public assistance and social services programs. Rapid and continuing technical advances have increased the dependence of state and local agencies on information systems. The value of VDSS information, software, hardware, telecommunications, and facilities is an important resource and must be protected.

1.2 Guiding Principles

The following principles guide the development and implementation of the ***VDSS Information Security Program***:

a. Information is:

   1. A *critical asset* that shall be *protected*; and

   2. *Restricted* to *authorized personnel* for *official use*.

b. Information Security must be:

   1. A *cornerstone* of *maintaining public trust*;

   2. Managed to address both business and technology requirements;

   3. ***Risk****-based* and *cost-effective*;

   4. Aligned with VDSS priorities, prudent industry practices, and government requirements;

   5. Directed by policy but implemented by business owners; and

   6. *Everybody's responsibility*.

1.3 Purpose

The purpose of the ***VDSS Information Security Policy and Program Guide*** is to:

a. Promote information security awareness to individuals using VDSS systems and information;

b. Make each user aware of their duty to protect VDSS information and information processing systems;

c. Ensure the ***confidentiality*** of VDSS information by protecting VDSS information and information systems against *unauthorized* access or disclosure;

d. Maintain the ***integrity*** of VDSS data by controlling who can add, modify, or delete it;

e. Meet requirements for ***availability*** of information and information systems, allowing VDSS the ability to provide services and benefits to its customers;

f. Reduce the ***risk*** of data loss by accidental or intentional modification, disclosure, or destruction; and

g. Preserve VDSS rights and remedies in the event of such a loss.

1.4 Statement of the *VDSS Information Security Program*

The Commissioner is responsible for the security of VDSS data, including case records and documents containing client or ***confidential***/***sensitive*** information, and for taking appropriate steps to secure VDSS information systems and data through the ***VDSS Information Security Program***. This program and related policies and standards provide the minimum security requirements that apply to all VDSS divisions/directorates/offices/districts/regions and Local Departments of Social Services (LDSS). Effective security is a team effort involving the participation and support of every user who interacts with VDSS data and information systems. It is the responsibility of every user to know these policies and to conduct their activities accordingly. Exceptions to this program and related policies and standards must be clearly documented, reviewed, and approved by the Commissioner or the VDSS Chief Information Security Officer (CISO) as appropriate.

The function of the ***VDSS Information Security Program*** is to protect VDSS information assets from credible threats, whether internal or external, deliberate or accidental. It is the policy of VDSS to use all reasonable security control measures to:

a. Ensure the ***confidentiality***, ***availability***, and ***integrity*** of data and systems;

b. Meet federal, state, and other regulatory and legislative requirements; and

c. Ensure business continuity in the event of any type of business interruption.

Violations of the ***VDSS Information Security Program*** must be reported to the appropriate VDSS State/Local Security Officer, Division Director, Regional Director, LDSS Director and the VDSS CISO. Depending on the severity, an employee who violates these policies may receive a Standards of Conduct notice. Violations of state and local laws will be reported to the appropriate law enforcement authorities. Prosecuting action may be undertaken if a person knowingly and intentionally violates any local, state, or federal laws or uses any VDSS-related information, information processing systems, or equipment for fraudulent, extortive, or destructive purposes.

Security measures must be taken to guard against *unauthorized* access to, alteration, disclosure, or destruction of data and information systems. This also includes accidental loss or destruction. In the case of lost or missing computer equipment or software, notification must also be made immediately to the VDSS CISO.

Related References:

Commonwealth of Virginia Information Security Program and Standard Exception Request (.doc)

Standards of Conduct, Department of Human Resource Management (.pdf)

2. Roles and Responsibilities

2.1 Policy

VDSS and LDSS must have an effective security administration function in place. For the ***VDSS Information Security Program*** to be effective, someone in each VDSS division/directorate/office/district/region and LDSS should be assigned the responsibility for administering the ***VDSS Information Security Program*** in their unit. The individual selected should be cognizant of data processing and information security fundamentals, and possess sufficient abilities to understand, implement and enforce information security policies and procedures.

VDSS operates with distributed security architecture. There are approximately 150 state and local VDSS offices located throughout the Commonwealth of Virginia (COV). Each VDSS division/directorate/office/district/region and LDSS must designate a ***Primary State/Local Security Officer*** and at least one ***Backup State/Local Security Officer*** whose responsibility is to ensure compliance with the ***VDSS Information Security Program***. The State/Local Security Officers are responsible for administering the users within their respective offices to include adding/removing users and modifying access privileges. The VDSS Information Security and Risk Management (ISRM) Office oversees the ***VDSS Information Security Program*** and provides administration for the Primary State/Local Security Officers and their backups.

2.2 Commissioner

The Commissioner is responsible for the security of VDSS information systems and data including case records and documents containing client or ***confidential*** information. The Commissioner, through the ISRM Office, is responsible for assuring that the ***VDSS Information Security Program*** is developed and distributed to all VDSS divisions/directorates/offices/districts/regions and LDSS staff, contractors, vendors, and other persons and organizations that have a need to use VDSS-related information and information processing systems. The Commissioner is responsible for final interpretation of this ***VDSS Information Security Policy and Program Guide***. The Commissioner delegates authority for the approval of related information security policies and procedures (See Section 8) to the VDSS CISO.

2.3 VDSS Chief Information Security Officer (CISO)

The VDSS CISO is responsible for developing and managing the ***VDSS Information Security Program***.

The VDSS CISO duties are as follows:

a. Develop and manage an ***Information Security Program*** that meets or exceeds the requirements of COV information security policies and standards in a manner commensurate with ***risk***;

b. Develop and maintain an ***Information Security Awareness Training Program*** for VDSS divisions/directorates/offices/districts/regions and LDSS staff, including contractors, student interns, volunteers, and service providers;

c. Coordinate and provide information security information to the COV CISO as required;

d. Implement and maintain the appropriate balance of protective, detective, and corrective controls for VDSS information systems commensurate with data ***sensitivity***, ***risk***, and ***system criticality***;

e. Mitigate and report all ***Information Security Incidents*** in accordance with the *Code of Virginia § 2.2-603* (Authority of agency directors), the Virginia Information Technologies Agency (VITA), federal requirements, and all other applicable obligations and take appropriate actions to prevent recurrence;

f. Maintain liaison with the COV CISO;

g. Verify and validate that all VDSS information systems and data are classified for ***sensitivity***;

h. Approve related information security policies and procedures associated with the ***VDSS Information Security Policy and Program Guide***; and

i. Publish components of the ***VDSS Information Security Program*** in multiple formats including but not limited to Portable Document Format (PDF), Word, and Hypertext Markup Language (HTML).

2.4 Information Security and Risk Management (ISRM) Office (Central Security Office)

The VDSS ISRM Office is responsible for providing technical information, security assistance, and fostering and overseeing the ***VDSS Information Security Program***. Specific responsibilities are as follows:

a. Provide technical assistance to VDSS divisions/directorates/offices/districts/regions and LDSS in developing, implementing, and administering their ***Information Security Programs*** and procedures;

b. Develop, maintain, and disseminate information security policies, standards and guidelines, ensuring their consistent interpretation and implementation throughout VDSS divisions/directorates/offices/districts/regions and LDSS;

c. Participate in VDSS system development activities to ensure an appropriate level of ***security***, ***confidentiality*** and ***availability*** is provided to VDSS systems;

d. Assist business areas to conduct Business Impact Analyses (BIAs) and Risk Assessments (RAs) for VDSS information systems;

e. Review ***Information Security Incident Reports*** and coordinate Corrective Actions (CAs) to prevent similar occurrences;

f. Investigate alleged security breaches; and

g. Administer access privileges for *ALL* contract employees.

Note: The Commissioner and the VDSS CISO reserve the right and may assign other responsibilities as required to the ISRM Office.

2.5 State/Local Security Officers

Primary and Backup State/Local Security Officer Appointments must be appointed by the appropriate Director/Designee. In order to maintain continuity of business operations, at least one Primary State/Local Security Officer and at least one Backup State/Local Security Officer should be appointed for each Division/Local office. Offices should appropriately appoint Backup State/Local Security Officers to support their needs. State/Local Security Officers serve as the Point of Contact (POC) for all security-related matters. State/Local Security Officers, appointed by their director, are authorized by this ***VDSS Information Security Policy and Program Guide*** to make decisions regarding the protection of VDSS information, resources, and user access privileges to ensure VDSS information and resources are protected from misuse or abuse.

The State/Local Security Officer Change Request Form should be sent from the Director to security@dss.virginia.gov.

State/Local Security Officers are responsible to:

a. Satisfactorily complete Local Security Officer training within 30 days of appointment and retake Local Security Officer training once every 3 years thereafter;

b. Administer user access privileges to VDSS information systems and resources;

c. ***NOT*** administer access privileges for contract employees;

d. Verify the access privileges of active employees *annually for each Information System* -

OASIS, LETS, VaCMS, APECS/iAPECS and every other role based access system (i.e., ASAPS, CRS, etc.).

e. Communicate security-related events to the VDSS CISO;

f. Ensure local staff members complete the ***Information Security Awareness and Federal Safeguards Training*** courses annually; and

g. Remove VDSS information system access for employees within three business days of change of responsibilities or separation.

Note: Personnel account transfers are not technically possible between Localities. Accounts must be deleted at old agency, and new accounts must be created within the new agency. Supervisors will need to complete new access forms.

Related Reference:

State/Local Security Officer Change Request Form (.docx)

2.6 LDSS/VDSS Division Directors - Approval requirements

LDSS/VDSS Division Directors are responsible to:

a. Request firewall changes;

b. Submit Administrative Access (AA) requests;

c. Submit Blue Coat and Audit Log requests;

d. Appoint Primary and Backup State/Local Security Officers (see State/Local Security Officers Procedures Manual);

e. Approve SPIDeR access;

f. Approve Non-VDSS Software requests; and

g. Delegate in writing a designated person who can approve Non-VDSS provided Software requests.

Note: If the Local Director is not available to submit/approve the request, then the approval of the Regional Director is required.

Related References:

See additional responsibilities – Section 2.7 Management

Related forms and procedures are on the ISRM Division SPARK website

2.7 Management

Managers at all levels are responsible for the security of VDSS Information systems and data, including case records and documents containing ***client*** or ***confidential*** information under their jurisdiction. They shall take all reasonable actions to provide adequate security and to escalate problems, requirements, and matters related to information security to the highest level necessary for resolution.

Division/directorate/office/district/regional management and LDSS directors are responsible to:

a. Appoint Primary and Backup State/Local Security Officers. Directors cannot be State/Local Security Officers because of conflict with ***separation of duties***. In order to maintain continuity of business operations, one Primary State/Local Security Officer and at least one Backup State/Local Security Officer should be trained and appointed for each Division/Local office.

b. Implement and enforce procedures within their units which ensure compliance with VDSS information security policies and standards;

c. Ensure violations or suspected violations of the ***VDSS Information Security Program*** are reported to the VDSS CISO; and

d. Ensure that all users of VDSS information and information systems are made aware of VDSS information security policies and standards and receive continuing ***Information Security Awareness Training***.

2.8 System Owner (VDSS Division Directors)

The System Owner is the VDSS manager responsible for making system-related development and maintenance decisions and establishing priorities. With respect to information security, the System Owner's responsibilities include the following:

a. Require new employees complete ***Initial Information Technology Security Awareness Training*** in the Knowledge Center prior to, or as soon as practicable after, receiving access to the system, but within the first 30 days of employment;

b. Require that all information system users complete the required ***Annual Information Security Awareness Training*** within the deadlines set by the ISRM Office;

c. Manage system ***risk*** and develop additional information security policies, standards, and guidelines required to protect the system in a manner commensurate with ***risk***;

d. Maintain compliance with VDSS information security policies, standards, and guidelines in all information system activities;

e. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system; and

f. Designate a System Administrator for the system if the system is not administered by the Information Technology Partnership - currently Virginia Information Technologies Agency/Northrop Grumman (VITA/NG).

2.9 Data Owner

The Data Owner is the VDSS manager responsible for the policy and practice decisions regarding data, including case records and documents containing ***client*** or ***confidential*** information. The Data Owner is responsible for the following:

a. Evaluate and classify ***sensitivity*** of the data with the assistance of the VDSS CISO;

b. Define protection requirements for the data based on the ***sensitivity*** of the data, any legal or regulatory requirements, and business needs with the assistance of the VDSS CISO;

c. Communicate data protection requirements to the System Owner;

d. Define requirements for access to the data; and

e. Approve Firewall requests.

2.10 Local Social Service Directors

LDSS Directors that enter data supplied by VDSS into local systems are responsible for the security of the local information systems and data contained therein. The LDSS Director is responsible for assuring that the ***VDSS Information Security Policy and Program Guide*** is distributed to all LDSS staff, contractors, vendors, and other persons and organizations that use local systems that process or store VDSS-provided information. The LDSS Director is responsible for final interpretation of local information security policies and procedures and will provide to the VDSS ISRM Office copies of all local information security policies and procedures.

The LDSS Director's data ownership responsibilities include:

a. Establish and maintain an ***Information Security Program*** for local systems that process or store VDSS-provided information (i.e., Harmony, EZ-filer) that includes:

    1. Information security policies and standards distributed to all individuals who use local systems that process or store VDSS-provided information; and

    2. An ***Information Security Awareness Training Program*** relevant to local systems.

b. Provide physical and logical ***separation of duties*** by ensuring no one person that has the ability to influence funds has sole control of ***sensitive*** processes.

2.11 All Personnel

All personnel, including VDSS employees, LDSS employees, contractors, volunteers, student interns, business partners, and any other users of VDSS information systems and resources are responsible for the following:

a. Read the ***VDSS Information Security Policy and Program Guide, the VDSS Information Resource Acceptable Use Policy*** and related information security policies, standards and procedures;

b. Read and sign the ***VDSS Information Security – Policy Acknowledgement*** form;

c. Comply with the ***VDSS Information Security Program***;

d. Do everything reasonably within their power to ensure that the ***VDSS Information Security Program*** is implemented, maintained, and enforced;

e. Report breaches of information security, actual or suspected, to the VDSS CISO and to appropriate management;

f. Take reasonable and prudent steps to protect the security of information systems and data to which they have access; and

g. Complete required ***Information Security Awareness Training*** as required within specified deadlines.

    1. ***Initial Information Security Awareness Training*** must be completed within 30 days of employment. Employees who are transferred between localities are required to complete the ***Initial Information Security Awareness Training*** within 30 days of the transfer.

    2. ***Annual Information Security Awareness Training*** must be completed within the deadline as broadcast by the ISRM Office yearly.

    3. ***Local Security Officer Training*** must be completed within 30 days of appointment and once every 3 years thereafter.

Related References:

VDSS Information Resource Acceptable Use Policy (.pdf)

VDSS Information Security - Policy Acknowledgement (.pdf)

2.12 System Administrator

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrators assist agency management in the day-to-day administration of VDSS information systems, and implement security controls and other requirements of the ***VDSS Information Security Program*** on information systems for which the System Administrator has been assigned responsibility.

The Division of Information Systems (DIS) and VITA are the System Administrators.

2.13 Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

a. Protect the data in their possession from *unauthorized* access, alteration, or destruction;

b. Establish, monitor, and operate Information systems in a manner consistent with COV information security policies, standards, and procedures; and

c. Provide Data Owners with reports, when necessary and applicable.

Note: NG is the Data Custodian for all VDSS data that resides on VITA/NG managed devices.

2.14 Communications with the ISRM Office

The Central Security Office (VDSS ISRM) provides support for approximately 150 state and local VDSS offices located throughout the Commonwealth. When contacting Security, please email security@dss.virginia.gov. Contacting individuals increases response time and doesn't allow back-up assistance on issues. Members of the Central Security Office monitor ***all*** incoming email messages sent to security@dss.virginia.gov. Most requests are processed on a First In, First Out basis. Time-***sensitive***, urgent, and high priority requests are processed as required. Include a ***descriptive subject line*** with ***every*** email. Not providing a ***descriptive subject line*** delays efficient processing. Name documents with descriptions when sending attachments and/or forms to the Central Security Office. For example, save Administrative Account request forms as Last Name First Name – Admin Rights – mmddyy.docx. The Central Security Office does NOT use a ticket system.

Examples of acceptable ***descriptive subject lines***:

ADAPT – First Name Last Name

APECS/iAPECS– First Name Last Name

Admin Account - First Name Last Name

Data Warehouse– First Name Last Name

Dual Factor Token - First Name Last Name

Encrypted Email – First Name Last Name

Guest Wireless - First Name Last Name

Password reset – Name of Application - First Name Last Name
(Example: Password reset – P16 or Password reset – LDAP)

CIPPS - First Name Last Name

Security Officer change – Name of Locality

Separation & Transfer Checklist – First Name Last Name

VaCMS- MAGI – First Name Last Name

Examples of acceptable ***descriptive document titles***:

Last Name First Name – Admin Rights – mmddyy.docx

Last Name First Name – ADAPT - mmddyy.docx

Last Name First Name – Data Warehouse - mmddyy.docx

Last Name First Name – Encrypted Email.doc

Last Name First Name – EPPIC - mmddyy.pdf

Last Name First Name – SPIDeR - mmddyy.docx

Last Name First Name VaCMS - mmddyy.docx

Remember:

- When contacting the Central Security Office, please email security@dss.virginia.gov.
- Please include a ***descriptive subject line*** in each communication.
- Name forms sent as attachments with ***descriptive document titles***.

2.15 Shared Support and Full Support Agency IT Management

In shared support agencies, the local IT department is responsible to load the VITA-approved desktop image. IT support work in shared support agencies is done by local, county, or city IT shop.

For full support agencies, VITA loads and manages the desktop image. IT support work in a full support agency is performed remotely or onsite by VITA or DIS IT staff.

3. Laws and Penalties

Privacy Act of 1974. Establishes a Code of Fair Information Practice that governs the collection, maintenance, use, and dissemination of ***Personally Identifiable Information (PII)*** about individuals that is maintained in systems of records by Federal Agencies. Provides that *unauthorized* access to, or disclosure of, ***PII*** in any manner to any person or agency not entitled to receive it is a misdemeanor. Violators are subject to a fine of not more than $5,000.

Internal Revenue Code (IRC 7213 & 7431). No employee of the federal, state, or local government shall unlawfully inspect and/or disclose taxpayer information. Provides that *unauthorized* disclosure of any information provided by the Internal Revenue Service (IRS) is a felony punishable by a fine not to exceed $5,000 or imprisonment for not more than 5 years, or both. Taxpayers may also bring civil action for damages sustained by the plaintiff as a result of such *unauthorized* disclosure.

Freedom of Information Act (FOIA). Establishes a "right-to-know" legal process by which requests may be made for government-held information, to be received freely or at minimal cost, barring standard exceptions. This act opens agency records to the public but requires the agency to ensure that policies and procedures are in place to review requests for information and deny release of ***protected*** and ***sensitive*** information. It provides for a civil penalty of up to $1,000 for knowing and willful violations.

Health Insurance Portability and Accountability Act (HIPAA) of 1996. HIPAA exists to protect the health information of citizens called Protected Health Information or PHI. The Enforcement Rule of HIPAA sets civil money penalties for violating HIPAA rules and establishes procedures for investigations and hearings for HIPAA violations. The Health Information Technology for Economic and Clinical Health Act (HITECH Act) extends the complete ***privacy*** and security provisions of HIPAA in 2009 to business associates of covered entities. VDSS and the LDSS are exempt from implementing HIPAA-related controls and requisite policies/procedures, particularly as they relate to the receipt and use of Department of Medical Assistance Services (DMAS) generated PHI.

Related References:

Code of Virginia § 2.2-3700. - FOIA.

Code of Virginia § 2.2-3803. - Administration of systems including personal information; Internet ***privacy*** policy; exceptions.

Code of Virginia § 2.2-3806. - Rights of data subjects.

Code of Virginia § 2.2-3815. - Access to social security numbers prohibited; exceptions.

Code of Virginia Title 63.2 - Welfare (Social Services).

Code of Virginia § 63.2-102. - Allowing access to records and information for public assistance programs and child support enforcement; penalty.

Code of Virginia § 63.2-103. - Confidential records and information concerning child support enforcement.

Code of Virginia § 63.2-104. - Confidential records and information concerning social services; penalty.

Code of Virginia § 63.2-104.1. - Confidentiality of records of persons receiving domestic and sexual violence services.

Code of Virginia § 63.2-105. - Confidential records and information concerning social services; child-protective services and child-placing agencies.

Code of Virginia § 63.2-405. - Provisions for determination of eligibility for medical care and medical assistance; provision of social services; regulations.

Code of Virginia § 63.2-501. - Application for assistance.

Federal Code § 7 CFR 272.1(c); - Disclosure.

Federal Code § 42 CFR 431.305 – Types of information to be safeguarded.

Federal Code § 42 CFR 431.306 – Release of information.

Federal Code § 42 CFR 433.138 – Identifying liable third parties.

Federal Code § 45 CFR 303.21 – Safeguarding and disclosure of confidential information.

Federal Code § 303.105 - Procedures for making information available to consumer reporting agencies.

Health Insurance Portability and Accountability Act (HIPAA) of 1996

26 U.S. Code § 6103 - Confidentiality and disclosure of returns and return information.

IRS Publication 1075 (.pdf) – Tax Information Security Guidelines for Federal, State and Local Agencies.

26 U.S. Code § 7213 – *Unauthorized* disclosure of information.

26 U.S. Code § 7431 – Civil damages for *unauthorized* inspection or disclosure of returns and return information.

ITRM Policies, Standards and Guidelines

Privacy Act of 1974 5 U.S.C. § 552a

Social Security Program Rules

Standards of Conduct, Department of Human Resource Management (.pdf)

Temporary Assistance for Needy Families (TANF) Manual 103.1 (1/20/97), Purpose of Safeguarding of Information and Scope of Regulations

USDA/FNS 7 CFR 72.1 (c), 27.1 (d), Disclosure of Information

VDSS/DCSE Manual, Chapter 2 (11/1/96), Confidentiality/Information Release

VDSS Medicaid Manual

Virginia Administrative Code 12VAC30-20-90.– Confidentiality and disclosure of information concerning Medicaid applicants and recipients.

4. Information Security Program

Information Security Programs must include protective measures and procedures to ensure that the appropriate levels of ***confidentiality***, ***integrity***, and ***availability*** of data, information, and systems are sustainable. The specific structure of an agency's Information Security Program will vary depending on the scope and nature of the information technology resources and ***sensitive*** information for which the agency is responsible.

A good Information Security Program should include documented policies and procedures that support the mission of the agency and is derived from industry best practices, and if applicable, the information security policies and standards of the COV and the federal government.

The VDSS CISO is charged with developing and administering the ***VDSS Information Security Program*** in a manner that meets VDSS business needs, protects Information systems and data in a manner commensurate with data ***sensitivity*** and ***risk***, and, at a minimum, meets the requirements of COV information security policies and standards.

4.1 Risk Management (RM)

Risk Management (RM) is the process of identifying and ensuring the protection of **sensitive** information and data received, processed, shared, and stored by VDSS.

COV requires all agencies to evaluate agency-owned Information systems that contain ***sensitive*** data at least once every three years via an IT Risk Assessment (RA). VDSS System Owners, Data Owners and ISRM will work together to complete RAs as a central component of the VDSS Information Security Program. The RA should evaluate ***risks*** and vulnerabilities and adopt mitigation steps (processes, procedures, hardware, software, etc.) to manage, minimize, eliminate or formally accept the risks if unable to mitigate them. All aspects of the RA process will consider ***confidentiality***, ***availability,*** and ***integrity*** of systems and data.

VDSS System and Data owners should be familiar with the VDSS Risk Assessment Policy. Data owners must perform a data ***sensitivity*** review of all systems which they use during the normal course of delivering benefits and services to the citizenry. For new systems or significant enhancements to existing systems, this data ***sensitivity*** review must be performed. The components of a RA include the Business Impact Analysis (BIA), Data/System Classification, Information Security Audits, and the System Security Plan (SSP).

If you are performing a RA, conform to VDSS and VITA RA procedures and IRS requirements stated in Publication 1075.

Related References:

COV IT Risk Management Standard SEC520-00 (.pdf)

COV Information Security Standard SEC501 (.pdf)

Government Data Collection & Dissemination Practices Act (GDCDPA) – disclosure of personal information.

IRS Publication 1075 (.pdf) – Tax Information Security Guidelines for Federal, State and Local Agencies.

VDSS Nondisclosure Agreement (.pdf)

4.1.1 *Sensitive* Data Definition

The Commonwealth of Virginia (COV) defines ***sensitive*** data as follows:

> "Any data of which the compromise with respect to ***confidentiality***, ***integrity***, and/or ***availability*** could have a material adverse effect on COV interests, the conduct of Agency programs, or the ***privacy*** to which individuals are entitled."

Data is deemed ***sensitive*** based on the following three criteria:

- ***Confidentiality*** - This addresses ***sensitivity*** to ***unauthorized disclosure***.

  Examples include:

  - Improper disclosure of individual client participation in certain benefit programs, such as Temporary Assistance for Needy Families (TANF) and Supplemental Nutrition Assistance Program (SNAP), to non-VDSS/LDSS sources;
  - Workers querying Application Benefit Delivery Automation Project (ADAPT) to determine a family member's status of a benefits application; and
  - Principle of ***Least Privilege*** for access and use is violated by worker access being provided beyond the minimum level of data, functions, and capabilities necessary to perform a user's duties.

- ***Integrity*** - This addresses ***sensitivity*** to ***unauthorized modification***.

  Examples include:

  - Changing citizen-level information on clients outside of the case worker's caseload; and
  - Approving benefits for a client where the same worker determined the client's eligibility (improper ***separation of duties***).

- ***Availability*** - This addresses ***sensitivity*** to outages, such as those determined by the BIA.

Examples include:

- VDSS email system will not be available in a disaster if the email provider is rendered inoperative and the email system is not backed up; and

- Disaster Supplemental Nutrition Assistance Program (DSNAP) is required to be functional in the event of a declared emergency.

It is in the best interest of VDSS to ensure that data being collected, maintained, or accessed is protected. To ensure COV standards are met, it is imperative that VDSS define ***sensitive*** information in a consistent manner across all VDSS divisions/directorates/offices/districts/regions and LDSS.

The following information/data is considered "***sensitive*** information":

- Third-party confidential information (both sent and received);
- ***PII*** (anything that could be used to identify a specific person) as covered by the GDCDPA;
- Federal Tax Information (***FTI***) that originated from the Internal Revenue Service (IRS), Social Security Administration (SSA), or U.S. Department of Labor; and
- Commissioner's working papers or correspondences used for deliberative purposes and not otherwise open to the public.

Other types of information should be discussed with the VDSS CISO to determine the appropriate security level and how that information should be classified.

Note: If in doubt about a non-disclosure issue, contact the VDSS CISO to determine the appropriate security level and whether a non-disclosure agreement is required. If there are concerns and potential legal issues, the VDSS CISO should contact legal counsel for further interpretation before action is taken. This step will avoid a potential interruption in VDSS business.

4.1.2 Business Impact Analysis

A critical component of the business continuity and risk assessment program is the Business Impact Analysis (BIA). A BIA is a process designed to prioritize business functions by assessing their potential quantitative (financial) and qualitative (non-financial) impact that might result if VDSS experiences a business continuity event (i.e., an interruption of significant duration). BIAs provide the foundation to any viable business continuity program.

The VDSS BIA provides a prioritized list of major business functions along with a strategy to sustain, or recover from, any type of disruption. Other benefits are identification of any known or potential ***risks***, which will be fed into subsequent RAs. All information gathered is used to revise VDSS Continuity Plans.

The VDSS Business Impact Analysis Policy describes the processes, procedures, and roles of the staff involved with BIAs.

4.1.3 Information System and Data *Sensitivity* Classification

VDSS information systems and data have been classified according to their ***sensitivity*** with respect to ***confidentiality***, ***integrity***, and ***availability***. The VDSS Information System and Data Classification Policy creates the processes, procedures and roles that define how the agency accomplishes System and Data classification.

4.1.4 *Sensitive* Information System Inventory and Definition

Each VDSS system has been documented, including its ownership and boundaries. Updated network diagrams are maintained and updated as changes occur. At least annually, an inventory that contains a listing of all programs and information systems identified as collecting, using, maintaining, or sharing ***FTI*** must be developed/reviewed and provided to the VDSS CISO.

Related Reference:

IRS Publication 1075 (.pdf) – Tax Information Security Guidelines for Federal, State and Local Agencies.

4.1.5 Risk Assessment (RA)

Based on the results of the BIA, the Risk Assessment (RA) identifies the risks that could compromise the ability of VDSS to perform its critical business functions. RAs will be conducted for all VDSS-owned critical information systems classified as ***sensitive***. RAs delineate the steps VDSS must take for each information system classified as ***sensitive*** to:

- Identify potential threats to the information system and the environment in which it operates;
- Determine the likelihood that identified threats will materialize;
- Identify and evaluate vulnerabilities; and
- Determine the loss impact if one or more vulnerabilities are exploited by a potential threat.

This is achieved by:

- Identifying information systems that contain ***sensitive*** information and, thus, require ongoing RA reviews;
- Examining information system documentation, especially security measures included in its design;

- Examining access controls in place to protect ***sensitive*** data;
- Collecting information via interview and questionnaires regarding ***confidentiality***, ***integrity***, and ***availability*** controls in place versus what is deemed to be needed; and
- Writing a RA report for management review that includes findings and recommendations to mitigate identified ***risks*** and vulnerabilities.

4.1.6 IRS Data

4.1.6. a. Definition of Federal Tax Information (*FTI*)

- ***FTI*** is any tax return or tax return information **received from the IRS or secondary source**, such as SSA, Federal Office of Child Support Enforcement or Bureau of Fiscal Service. ***FTI*** includes any information created by the recipient that is derived from return or return information.
- ***FTI*** does not include information provided directly by the taxpayer or third parties.
- If the taxpayer or third party subsequently provides returns, return information, or other ***PII*** independently, the information is not ***FTI***, and cannot be considered as Federal Tax Information.
- ***FTI*** only becomes non IRS/SSA protected data when it is **overwritten** in the agency's records by another source of data, such as citizen provided.

4.1.6. b. Disclosure of *FTI* to Non-Paid Employees

- Access to ***FTI*** is strictly prohibited for non-paid employees, such as student interns, volunteers or any other type of non-paid employee.

4.1.6. c. Disclosure of *FTI* to Benefit Programs Contractors

- No officer or employee of any federal, state, or local agency administering certain programs under the Social Security Act, the Food Stamp Act of 1977, or Title 38, United States Code, or certain housing assistance programs is permitted to make further disclosures of ***FTI*** for any purpose.
- **Human services agencies may not contract for services that involve the disclosure of FTI to contractors. For accessing FTI, the IRS considers workers to be either employees or contractors. An employee is a worker that receives a W2 issued by the locality or State. The IRS considers everyone else a contractor as far as accessing FTI is concerned. This definition includes interns, volunteers, and VIEW workers, as well as workers that receive a 1099. Everyone falling under this broad definition of a contractor is prohibited from accessing FTI.**

- The following systems contain ***FTI***. As a result, contractors, student interns and volunteers are not allowed to have access to them: SPIDeR-ADAPT, SPIDeR-MMIS, ADAPT, and Data Warehouse.

- Contractors have been given permission to access Energy Assistance System (EAS) as this benefit program does not use IRS provided data to determine eligibility. All workers are advised to ensure they follow the Benefit Programs prescribed business process for determining eligibility for EAS and not use any non-authorized income source.

4.1.6. d. Access by Division of Child Support Enforcement (DCSE) Contractors

- In general, no officer or employee of any state and local child support enforcement agency can make further disclosures of ***FTI***.

- **However, limited information may be disclosed to agents or contractors of the agency** for the purpose of, and to the extent necessary in, establishing and collecting child support obligations and locating individuals owing such obligations.

- The information that may be disclosed for this purpose to an agent or a contractor is limited to:
    - The address;
    - Social Security Number of an individual with respect to whom child support obligations are sought to be established or enforced; and
    - The amount of any reduction under IRC 6402(c) in any overpayment otherwise payable to such individual.

- Tax refund offset payment information may not be disclosed by any federal, state, or local child support enforcement agency employee, representative, agent, or contractor into any court proceeding. To satisfy the re-disclosure prohibition, submit the payment date, whether the payment is voluntary or involuntary, and the payment amount for all payment sources (not just tax refund offset payments) into court proceedings.

4.1.6. e. Comingling of *FTI*

Comingling of ***FTI*** refers to having ***FTI*** and non-***FTI*** data residing on the same paper, electronic media, or data center.

- ***FTI*** must be kept separate from other information to the maximum extent possible to avoid inadvertent disclosures.

- Agencies should attempt to avoid maintaining ***FTI*** as part of their case files.

- In situations where physical separation is impractical, the file must be clearly labeled to indicate that ***FTI*** is included, and the file must be safeguarded.

- All ***FTI*** must be removed prior to releasing files to an individual or agency without authorized access to ***FTI***.

4.1.6. f. Data Sharing

- Agencies and subdivisions within an agency may be authorized to obtain the same ***FTI*** for different purposes, such as a state tax agency administering tax programs and a component human services agency administering benefit eligibility verification programs (IRC 6103[l][7]) or child support enforcement programs (IRC 6103[l][6]). **However, the IRC disclosure authority does not permit agencies or subdivisions of agencies to exchange or make subsequent disclosures of this information for another authorized purpose even within the agency.**

- In addition, unless specifically authorized by the IRC, agencies are not permitted to allow access to ***FTI*** to agents, representatives, or contractors.

- ***FTI*** cannot be accessed by agency employees, agents, representatives, or contractors located offshore—outside of United States territories, embassies or military installations.

- Further, ***FTI*** may not be received, processed, stored, transmitted, or disposed of by information technology (IT) systems located offshore.

- The agency must restrict the sharing/re-disclosure of ***FTI*** to only those authorized in IRC 6103 and as approved by the IRS Office of Safeguards.

4.1.6. g. *FTI* in Transit

When ***FTI*** is hand-carried by an individual in connection with a trip or in the course of daily activities, it must be kept with that individual and protected from *unauthorized* disclosure.

All paper and electronic ***FTI*** transported through the mail or courier/messenger service must be documented on a transmittal form and monitored to ensure that each shipment is properly and timely received and acknowledged. It must also be double-sealed; for example, one envelope within another envelope. The inner envelope must be marked “confidential” with some indication that only the designated official or delegate is authorized to open it. Using sealed boxes serves the same purpose as double-sealing and prevents anyone from viewing the contents thereof.

4.1.6. h. Faxing *FTI*

To fax any document containing ***FTI*** you must:

- ensure a trusted staff member is at both the sending and receiving fax machines;
- maintain broadcast lists and other preset numbers; and
- place fax machines in a secured area.

Be sure to include a cover sheet on fax transmissions that explicitly provides guidance to the recipient that includes:

- A notification of the ***sensitivity*** of the data and the need for protection; and
- A notification to unintended customer to telephone sender, calling collect if necessary report the disclosure of/and confirm the destruction of the information.

Misrouted faxes constitute an *unauthorized* disclosure of ***FTI*** and must be reported under the provisions of Publication 1075 section 10.0.

4.2 Continuity Planning (CP)

CP defines business processes and all necessary supporting items, such as information systems/applications/data/people, that are needed if an event occurs that renders VDSS unable to operate.
The CP includes Emergency Response Plans, Business Continuity Plans, IT Disaster Recovery (ITDR) Plans, and Information System and Data Backup and Restoration Plans. The CP is explained further in the VDSS Business and Information System Continuity Planning Policy.

The results of CP are the Agency Continuity Plan and Division-level Continuity Plans. The VDSS Continuity Plan is mandated by the Virginia Department of Emergency Management (VDEM) and must be submitted to them annually, using the official COV template, by April 1st of each year.

4.2.1 Emergency Response Plans

The VDSS Emergency Response Plan is in development and coordinated by the VDSS Offices of General Services, Emergency Management, and the ISRM Business Continuity Manager. It will include information such as evacuation procedures, first aid/cardiopulmonary resuscitation (CPR), and shelter-in-place, etc. (i.e., all information needed for the first hours following any type of disruption).

4.2.2 Business CP

All executive agencies within the COV are required to submit Continuity Plans to VDEM annually no later than April 1st. This requirement is supported by Executive Order (EO) #41 (2011) entitled "Continuing Preparedness Initiatives in State Government and Affirmation of the Commonwealth of Virginia Emergency Operations Plan."

Business Continuity Plans are activated during or immediately after the Emergency Response Plans are in use. Per requirements by VDEM, the VDSS Continuity Plan contains VDSS Mission Essential Functions (MEFs) and Primary Business Functions (PBFs) that support the MEFs. It also includes details for how, when, why, where, and by whom the MEFs and PBFs will be recovered in a disaster situation. VDSS has a Recovery Leadership Team (RLT) that will direct the recovery efforts until the primary facility (or a new one) is available for occupancy.

Essential VDSS business functions are identified in the completion of the most recently approved BIA (described above). These functions may or may not be dependent upon IT resources.
In addition to the VDSS Continuity Plan, each Division within VDSS has its own Continuity Plan that mirrors the VDSS plan and further describes how each division will respond to an emergency and recover their business functions. Local Departments of Social Services should consult with their County Emergency Planners and develop a plan based on local directives.

4.2.3 IT Disaster Recovery (ITDR) Plans

ITDR planning is required by the COV *Information Security Program*. ITDR planning supports CP by defining specific policies, standards, procedures, and processes for restoring information systems and data that support mission essential business functions on a schedule that supports the agency's mission requirements. Based on identified RTOs[1] and Recovery Point Objectives (RPOs)[2], the ITDR plan ensures that information systems/applications/data can be recovered as required.

The VDSS DIS is responsible for creating and maintaining the VDSS ITDR plan, working in conjunction with the ISRM Business Continuity Manager to sync recovery of information systems to priorities established in the BIA to accommodate RTOs and RPOs. DIS works closely with VITA/NG to accomplish ITDR planning.

[1] RTO (Recovery Time Objective): The period of time within which systems, applications, or business functions must be recovered after an outage, enumerated in business time (e.g., within one business day) or elapsed time (e.g., within 48-72 hours).
[2] RPO (Recovery Point Objective): Identifies the amount of data loss that can be tolerated (e.g., two hours) that dictates how often the data must be backed up.

4.2.4 Information System and Data Backup and Restoration Plans

Information system and data backup and restoration plans are components of the ITDR plan and, thus, the responsibility of the VDSS DIS. These plans must be implemented to create a backup plan, including standards and operational procedures, executed during a system backup. The plans correspond to the needs identified in the BIA. These plans include standards and operational procedures to be executed during system restoration. The information in these plans must directly correspond to agreements between VDSS and VITA/NG for backup and recovery services.

Related References:

COV Information Security Program SEC 519-00 (.pdf)

COV Information Security Standard SEC501 (.pdf)

Executive Order #41 - Continuing Preparedness Initiatives In State Government and Affirmation of the Commonwealth of Virginia Emergency Operations Plan.

IRS Publication 1075 (.pdf) – Tax Information Security Guidelines for Federal, State and Local Agencies.

VDEM Continuity Planning - Continuity of Operations is an effort within individual agencies to ensure they can continue to perform mission essential functions during a disruption of normal operations.

4.3 Information Systems Interoperability Security

The systems that can be accessed through Systems Partnering in a Demographic Repository (SPIDeR) are on a variety of technical platforms. Some of these systems belong to VDSS and some belong to the IRS, the SSA, the Virginia Employment Commission (VEC), the Division of Motor Vehicles (DMV) and others.

For LDSS staff, authorization to the SPIDeR system is determined and approved by the LDSS Director. All VDSS staff members need authorization from their Director. In both cases, access will only be approved if it is necessary to fulfill job responsibilities. All state and federal ***confidentiality*** rules apply when accessing the data.

Related Reference:

Section 4.11 Data Protection

4.4 Information System Application Security

Application security controls are in place to define the high level specifications for system applications for VDSS. During application planning, data is classified according to the ***sensitivity*** of the data. A RA is conducted before development begins and after planning is complete, if the data classification identifies the system as ***sensitive***. Early in the system development lifecycle, security requirements of the

application are identified and documented. The results of the data classification process are used to assess and finalize any encryption, authentication, access control, and logging requirements. Please refer to the VDSS Applications Development Security Requirements developed by the ISRM Office for specific application development, production and maintenance security requirements. All VDSS system development efforts (either new systems or significant modifications to existing systems) must involve the VDSS ISRM Office in all phases of system development.

Usage of VDSS systems is logged. This logging enables the VDSS ISRM Office to determine who did what, to what record, and when it was done. Viewing of ***FTI*** is also logged.

Related References:

Applications at VDSS

VDSS Applications Development Security Requirements Policy (.xlsm)

4.5 Remote Access – Dual Factor Authentication

VDSS uses the NG-provided Cisco virtual private network (VPN) client for remote access. Any remote access where ***FTI*** is accessed over a remote connection must be performed using multi-factor authentication, i.e., Dual Factor Authentication. ***FTI*** cannot be accessed remotely by agency employees, agents, representatives, nor can it be accessed by contractors located offshore – outside of the United States territories, embassies, or military installations. Further, ***FTI*** may not be received, processed, stored, transmitted, or disposed of by information systems located offshore.

An access request process has been developed for the Dual Factor Token. The Dual Factor Token form is sent as an attachment to the VDSS ISRM Office at security@dss.virginia.gov with the ***descriptive subject line***: "Dual Factor Token - First Name Last Name," and will normally be submitted/approved by the State/Local Security Officer, Manager or Director. Additional requirements include ***business justification***, what applications will be accessed and whether the token will be used for telecommuting. The security token and instructions will be provided to the employee or the approver.

- A soft token utilizes software on the computer to issue the token codes.
- A hard token (key fob) is a physical device that is used to issue the token codes.

The determination on whether a worker requires a soft or hard token is made by the Central Security Office Staff from the information provided on the Dual Factor Token request form.
Hard tokens cost approximately $150 each. Report lost, damaged, or missing hard tokens (key fobs) within 24 hours to security@dss.virginia.gov to ensure deactivation. The Central Security Office does not reassign hard tokens between workers without the token first being returned to the Central Security Office.

Return hard tokens via interoffice mail to the VDSS Information Security and Risk Management Office, 801 East Main Street, 7th Floor, Richmond, Virginia 23219.

Related References:

Dual Factor Token (.docx)

IRS Publication 1075 (.pdf) – Tax Information Security Guidelines for Federal, State and Local Agencies.

VDSS Information Resource Acceptable Use Policy (.pdf)

VPN Site-to-Site Change (.doc)

4.6 Wireless Security

Wireless transmissions of any data are extremely vulnerable to improper recovery or inadvertent access. Due to the relative ease in recovering these transmissions, specific security requirements are necessary. VDSS employees can use a variety of wireless access systems, and the most frequently used are discussed in the following sections. Any access not specifically addressed below is prohibited unless explicit permission is granted from the VDSS ISRM Office.

4.6.1 COV Wireless

The VDSS Home Office has added the capability that allows users with COV devices to connect the COV WLAN in all main conference rooms. This VITA/NG provided service meets COV security requirements. Users working on ***sensitive*** systems or projects over the WLAN should utilize 2-factor VPN as an additional layer of security. The WLAN will be scanned annually and is subject to VDSS sponsored penetration testing.

4.6.2 Guest Wireless

The VDSS Home Office has added the capability to provide visitors of VDSS Guest Internet access in all main conference rooms. This will provide Internet access only and not serve as a connection path to VDSS systems or to the COV network. A request for visitor's access to the Wireless Guest Network must be submitted by the VDSS sponsor of the visitor who can affirm the Visitor's business need for access. To ensure that access is established by the time of the visitor's arrival, please plan ahead and allow three to five business days for establishing the account and delivery of user id, password, and instructions.

The responsible sponsor should complete the ***Guest Wireless Internet Access Request*** and send the completed form electronically to guest.wireless@dss.virginia.gov with the ***descriptive subject line***

"Guest Wireless Access – First Name Last Name." When the ISRM Office grants access, they will email the Visitor the "Guest User Details" to the email account included on the access request. This email will provide the user id and password, the Terms of Use, and instructions for logging into the wireless network. Included in the Terms of Use will be the statement "by using this account I agree to abide by Terms of Use as provided."

Note:

- Other use of wireless communication is prohibited without express written consent from the VDSS CISO.
- VDSS and LDSS employees may sponsor their own Guest Wireless Account requests.
- The business need for access is required on the Guest Wireless Internet Access Request form.
- NG Guest Wireless accounts are limited by the system to a maximum duration of 90 days. Each VDSS employee may submit their own renewal form/request for continued access in advance of the account end date.
- Shared accounts are NOT allowed.

Related Reference:

Guest Wireless Internet Access Request (.docx)

4.6.3 Wireless from Home or other Public Places

VDSS users need to ensure, when accessing external wireless connections, that the session is encrypted and appropriately secured.

Specific Wireless requirements are listed in COV Security Standard SEC 501. Before adding wireless access to any system, submit the plan for implementing this capability to the VDSS CISO for review and approval before any funds are expended. Any exceptions must be coordinated through the VDSS CISO and permissions explicitly granted.

Related References:

COV Information Security Standard SEC501 (.pdf)

Outlook Webmail - https://webmail.vita.virginia.gov/

4.6.4 Wireless in Regional/Local Offices

Wireless in local offices must comply with the same requirements as those deployed by VDSS. Any exceptions must be coordinated through the VDSS CISO and permissions explicitly granted. Specific wireless requirements are listed in COV Security Standard SEC 501. Before adding wireless access to any system, submit the plan for implementing this capability to the VDSS CISO for review and approval before any funds are expended.

4.7 Mobile Devices

According to the ***VDSS Information Resource Acceptable Use Policy,*** users may access their COV-provided email from any personal computer, smart phone, iPad, or other devices, using the Internet. Users who remotely access any other VDSS resources will use only VDSS-provided equipment that is configured, set up and maintained by VITA/NG technicians without modification or similar equipment provided by a locality that is not supported by the Commonwealth's partnership with NG. At a minimum the selection, implementation and use of mobile devices must include the elements outlined in the COV Mobile Device Security Policy. Mobile Devices purchased and owned by local governments to support LDSS operations are covered under this same approval as long as they subscribe to the same mobile device management as the VDSS-provided equipment. All mobile devices must be password protected.

The Enterprise Handheld Services (Non-Blackberry) or (EHS) is the approved mobile device management solution in the COV and VDSS. The secure mobile device management (MDM) solution is designed to reduce data loss on today's most popular iOS, Android, and Windows Phone mobile devices. All LDSS that use iPADs to access COV networks or applications need to use the approved EHS purchased through VITA or procured by your local government. This service should be ordered at the time of purchase or as an additional service to existing devices thru the current equipment management process managed by the VDSS IT Services Manager. A standard feature of this service is the ability to remotely wipe data from devices if they are lost or stolen. To subscribe to the service you must:
Open a ticket with the VCCC and have it assigned to the VDSS IT Services Manager group requesting a Work Request be submitted for Enterprise Handheld Services (Non-Blackberry).

> *Note: The use of non-COV owned mobile devices is expressly prohibited to access VDSS applications and networks. The only authorized use of personally owned devices is to access Webmail.*

Related Reference:

COV Mobile Device Security Policy (.pdf)

4.7.1 Bring Your Own Device (BYOD) Enterprise Handheld Services

VDSS employees whose supervisors approve the business need may use their personal mobile communications devices to securely access Commonwealth voice and email systems to conduct

official state business through VITA's Bring Your Own Device (BYOD) service. Only one "stipend-eligible" device is allowed per employee. This service is available only for devices with data plans to access COV email and network resources.

No access shall be granted to any VDSS information system on a BYOD including voice-only devices.

Department of Accounts (DOA) Requirements

The DOA policy requires that prior to providing a stipend to an employee who is authorized to use a non-Commonwealth owned mobile communications device, the employee's supervisor and the director shall sign the "COV Mobile Device Allowance Agreement."

The DOA has established provisions in the Commonwealth Accounting Policies and Procedures (CAPP) Manual that govern the terms under which agencies may provide stipends to employees as reimbursements for the use of non-Commonwealth owned mobile communications devices to conduct official business. See CAPP Manual, Volume 1 – Policies and Procedures, Topic: 50535, Mobile Device Provisions.

MBL-R-23 Maximum Allowed Reimbursement - The DOA policy establishes the maximum allowed reimbursement and how it shall be applied in order for the stipend to be provided in compliance with Commonwealth policies and federal Internal Revenue Service (IRS) income tax and withholding laws. The current maximum allowed reimbursement is $45.00 per month.

Requests to establish this connection must be submitted to the VCCC as a Service Request. Request the Ticket be assigned to the VDSS IT Services Manager. This will be processed by VDSS/DIS and the user notified when the device can be connected and will also provide the necessary steps the worker must take to make the connection.

Related References:

Commonwealth Accounting Policies and Procedures (CAPP) Manual

COV Mobile Device Allowance Agreement Form (.pdf)

Enterprise Architecture Standard (.pdf)

Mobile Communications Use Technical Topic Report (.pdf)

VDSS Information Systems Telecommunications Policy and Procedures (.pdf)

4.8 Logical Access Control

Logical access control requirements define the steps necessary to protect the ***confidentiality***, ***integrity***, and ***availability*** of VDSS systems and data against compromise. Logical access control requirements

identify the measures needed to verify that all information system users are who they say they are and that they are permitted to use the systems and data they are attempting to access. Logical access control defines requirements in the areas of Account Management, Password Management, and Remote Access.

The principle of ***Least Privilege*** must be followed for all employees who access VDSS systems. A basic principle in information security, ***Least Privilege***, holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

> *Note: No one can approve/implement access changes for themselves. In the case of a State/Local Security Officer updating SAMS, another State/Local Security Officer must make the access changes. SAMS was updated in 2012 to prevent a Division/Local Security Officer from changing their own access.*

4.8.1 Account Management

Account management standards and procedures must be implemented to ensure the steps necessary for requesting, granting, administering, and terminating accounts at VDSS are formalized. **ALL** Access Request Forms **must** be submitted electronically. The most current versions of the authorized Access Request Forms are located on SPARK under Forms on the ISRM section.

4.8.1. a. Non-Paid Employees

The LDSS should consider its volunteers, student interns, and various community organizations as non-paid employees to comply with Federal and State code restrictions on use/disclosure requirements if their local legal representative has approved the use of non-paid employees.

> *Note: This designation as a non-paid employee is only for data security/access purposes and is not intended to confer the rights that paid employees have, such as access to the grievance system or other benefits.*

Access to ***Federal Tax Information (FTI)*** is strictly prohibited for non-paid employees such as student interns, volunteers, or another type of non-paid employee. This means no access to ***sensitive*** systems including ADAPT, SPIDeR-ADAPT, SPIDeR-MMIS, and APECS/iAPECS. Access to email and OASIS is acceptable.

If the LDSS Office has approval to use non-paid employees, a ***Local Confidentiality/Non-Disclosure Agreement*** for the non-paid employee must be signed. This agreement must also be reviewed and approved by the local legal counsel. The agreement should include:

a. A statement of understanding the nature of the information they are being granted access to;

b. The limits of its use; and

c. An understanding of the legal penalties that *unauthorized* use and/or disclosure can be applied.

The LDSS should retain the ***Local Confidentiality/Non-Disclosure Agreement***, the ***VDSS Information Security - Policy Acknowledgement Form,*** and all Access Request Forms for the non-paid employee. The LDSS is advised to comply with standard retention schedules.

4.8.1. b. Approval Process Flow for VDSS Security Forms

1. The worker (or the supervisor) fills out the form and emails it to the supervisor.
2. The supervisor approves and forwards via email as noted on Access Request Form Instructions.

NOTE: Some access requires the Director to approve, while most only require the supervisor.

4.8.1. c. Supervisor Approval Checklist

- ✓ Verifies the email came from the employee.
- ✓ Provides the ***business justification*** for the access requested by the worker.

  Example: Employee is a Benefit Programs policy trainer and needs to train on both ADAPT and the program policies that use the ADAPT system.
- ✓ Renames the Access Request Form descriptively.

  Example: Last Name First Name -ADAPT – mmddyy ADAPT.docx.
- ✓ The Supervisor types in their name and the date on the form, saves it, and emails the form as appropriate to the routing on the particular form. *Please see the* ***Access Request Form*** *for specific instructions.* A descriptive subject line in the email should be included:

  Example: ADAPT – First Name Last Name

4.8.1. d. Director Approval Checklist

- ✓ Verifies the email came from the supervisor.
- ✓ Verifies the Access Request Form has a descriptive ***business justification*** and verify the access requested by the worker.
- ✓ The Director types in their name and the date on the Access Request Form and emails the Access Request Form to the State/Local Security Officer.

The State/Local Security Officer reviews the Access Request Form and sends via email to security@dss.virginia.gov.

> *Note: The Director **must approve and submit to the Central Security Office all** State/Local Security Officer changes including terminations, requests for Local administrative rights, SPIDeR access requests, firewall changes, Non-DSS Software Requests and Audit Log Bluecoat Requests.*

4.8.1. e. State/Local Security Officer Checklist

- ✓ Ensures that the Access Request Form is completely filled out.
- ✓ Verifies the ***business justification*** has been completed.
- ✓ Ensures that the email chain shows emails sent from the supervisor (to the Director, if required) and to the State/Local Security Officer with all names showing on the Access Request Form.
- ✓ The State/Local Security Officer saves the official local copy of the Access Request Form (suggest electronically).
- ✓ The State/Local Security Officer creates the access unless it is a contractor or unless instructed to do otherwise in the form's instructions.

The VDSS ISRM Office reviews and processes all properly documented and approved access requests.

> *Note: The Director **must approve and submit to the Central Security Office all** Security Officer changes, requests for Local Administrative rights, SPIDeR access requests, firewall changes, Non-DSS Software Requests and Audit Log Bluecoat Requests.*

Related Reference:

Access Request Forms are on SPARK

4.8.2 Password Management

Passwords are used in many ways to protect data, systems, and networks. They are used to authenticate users of operating systems and applications such as email, labor recording, and remote access. Passwords are also used to protect files and other stored information, such as password-protecting a single compressed file, a cryptographic key, or an encrypted hard drive. VDSS uses the Open Lightweight Directory Access Protocol (LDAP), an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.

Effective password management reduces the risk of compromise of password-based authentication systems. VDSS needs to protect the ***confidentiality***, ***integrity***, and ***availability*** of passwords so that all authorized users—and no unauthorized users—can use passwords successfully as needed. Data security controls ensure ***integrity*** and ***availability*** through measures like using access control lists to prevent

attackers from overwriting passwords and having secured backups of password files. Ensuring the ***confidentiality*** of passwords is considerably more challenging and involves a number of security controls along with decisions involving the characteristics of the passwords themselves. For example, requiring that passwords be long and complex makes it less likely that attackers will guess or crack them, but it also makes the passwords harder for users to remember, and thus more likely to be stored insecurely. This increases the likelihood that users will store their passwords insecurely and expose them to attackers.

VDSS has adopted ***strong password*** criteria. A ***strong password***:

- Is at least eight (8) characters;
- Does not contain the user name, a real name, or VDSS;
- Does not contain a dictionary word;
- Is significantly different from previous passwords;
- Contains uppercase and lowercase letters and alpha and numeric characters; and
- Cannot be reused except after 24 times using other passwords.

4.8.2.a. User Password Management Responsibilities

Users of VDSS systems:

- May not share passwords;
- May change passwords at will, but no more than once every 24 hours;
- Must change passwords every 90 days; and
- Must change compromised passwords.

Note: Legacy systems (i.e., ADAPT and APECS/iAPECS) still change passwords every 30 days.

4.8.2.b. Lost, Stolen, or Compromised Passwords

VDSS users must:

- Immediately report to the VDSS CISO the loss, theft, or compromise of passwords; and
- Immediately change their password, if compromised.

4.8.2.c. Expired Passwords and Password Resets

VDSS users must change passwords every 90 days. Legacy systems (i.e., ADAPT and APECS/iAPECS) still change passwords every 30 days. All accounts without activity after 90 days are locked and will require an email from supervisor indicating the account is necessary in order for a password reset. All accounts without activity after 180 days are disabled and require new access request forms to establish access.

The "3-strikes" security feature for LDAP accounts locks a worker's account after three (3) consecutive incorrect password attempts. The "3-strikes" feature applies to a worker's LDAP ID and controls access to many VDSS systems including SAMS, VaCMS, SPIDeR, ASAPS, and MWS. State/Local Security Officers will need to be contacted in order to reset passwords for locked LDAP accounts.

VDSS users are required to change the temporary reset password on first use.

Contact the DIS Help Desk for OASIS password resets.

P16 password resets – The request must be submitted to security@dsss.virginia.gov from the State/Local Security Officer.

LDAP password resets – The request must be submitted to security@dss.virginia.gov from the. State/Local Security Officer.

LDAP passwords can be reset by the designated State/Local Security Officers, the DIS Help desk or by emailing a request to security@dss.virginia.gov.

4.9 Firewalls

The VDSS DIS Firewall Change Request Form and approvals are required for all firewall changes. Each approver should type his/her name and forward to the next approver. The email string will serve as approval documentation. All firewall requests must be approved by the agency Director. The Business Owner is the final approver. The completed form should be submitted by the Business Owner (usually Director) electronically to security@dss.virignia.gov for processing.

Related Reference:

VDSS DIS Firewall Change Request Form (.docx)

4.10 Administrator Accounts (AA)

An Administrator Account (AA) is a privileged user account that lets you make changes that will affect other users and data. AA rights are granted **only** to currently trained State/Local Security Officers and their use is limited to adding printers, print drivers, and any other local applications approved by ISRM, such as Thomas Brothers or Harmony. VDSS DIS Support Center has remote capability to provide all of the services listed previously. Agency Directors who still have a business need for an AA account must

use the VITA Email Mailbox and Account Request Form using the TEMPLATE provided by the Central Security Office.

- Administrator Account requests must be approved by ***agency Directors***, and the request ***must*** be sent ***directly*** from his/her email account to security@dss.virginia.gov with a specific subject line required (Ex: Admin account – First Name Last Name). Only an ***agency Director*** can request or submit an AA account request. The ***VDSS State/Local Security Officers Procedures Manual*** describes the process for requesting AA accounts.

- Administrator passwords must be reset every 90 days. Accounts lock if not used in 90 days and are removed after 180 days of inactivity. The Central Security Office will review all AA accounts biannually with supervisors to determine if access is still needed;

- Shared AA accounts are ***NOT*** permitted.

- No one can request access for themselves.

- AA holders must abide by the ***VDSS Information Resource Acceptable Use Policy***. ISRM will revoke AA privileges if they have been used for unapproved or unauthorized purposes such as changing security settings, installing unapproved software, updating registry settings, and/or accessing other user's files.

Note: Shared support agencies do not use COV Administrative Accounts.

Related Reference:

VITA Email Mailbox and Account Request Form (.doc)

4.11 Data Protection

Data protection provides security safeguards for the processing and storing of data. This component of the ***VDSS Information Security Program*** outlines the methods that can be used to safeguard the data in a manner commensurate with the ***sensitivity*** and ***risk*** of the data stored. Data Protection includes requirements in the areas of media protection and encryption.

VDSS has seven (7) main systems that store and/or capture ***confidential*** information that users must safeguard against *unauthorized* disclosure and access.

Client information should not be comingled with FTI.

VDSS systems that store and/or capture ***confidential*** information:

- OASIS
- ADAPT

- APECS/iAPECS
- SPIDeR
- VaCMS
- EPPIC
- ASAPS

OASIS (Online Automated Services Information System) is an online case record system related to family services cases. The VDSS Division of Family Services promotes and supports the development of healthy families and helps protect Virginia's children and adults from abuse and neglect.

OASIS:

- Contains information relating to Child Protective Services, Foster Care and Adoption and is the system of record for these areas; and

- Contains some of the most ***sensitive*** and restricted data for use by VDSS/LDSS employees.

OASIS is also a primary source of data for federal, state and local child welfare agencies' reporting and planning efforts.

ADAPT (Application Benefit Delivery Automation Project) is used by Benefit Programs to provide an online case record, available statewide to authorized LDSS and home office users, of information related to family services cases.

APECS/iAPECS (Automated Program to Enforce Child Support) is the statewide automated system that supports the Commonwealth's child support enforcement program. APECS/iAPECS combines all types of child support cases within one integrated system, and it features both case management and financial management capabilities. It is certified by the federal Office of Child Support Enforcement (OCSE) as meeting all requirements mandated by the Family Support Act of 1988 and the Personal Responsibility and Work Opportunity Reconciliation Act of 1996.

SPIDeR (Systems Partnering in a Demographic Repository) is a system which not only acts as a repository for various VDSS publishing systems, but also provides access to other state and several federal agencies' citizen-level information. SPIDeR also publishes client-level information to various VDSS systems from the repository and it also reaches back to other systems and pushes data to recipient systems. Because of the data SPIDeR receives and handles, SPIDeR is considered a ***sensitive*** system which also contains federally-sourced data.

SPIDeR also provides pathways for users to directly inquire other COV agency information (such as that information available from DMV and VEC), as well as certain federal systems (such as SSA's SOLQ-I [SSA State Online Query]).

SPIDeR contains audit logging capabilities which capture all users' actions conducted within or through SPIDeR. The ISRM Office can pull audit logs for all SPIDeR users' activities and uses the audit logs to provide assurances regarding the access to and use of SPIDeR information by employees.
Access to SPIDeR is restricted to VDSS/LDSS employees only. **No contractors, volunteers, student interns, or other non-employees should have access to, or use of, SPIDeR** due to the ***sensitive*** and

federally-sourced information contained within SPIDeR. There are no provisions made within the various LDSS MOAs which allow contractors, volunteers, student interns, or other non-employees to access or use SPIDeR.

Systems Currently Partnered with ***SPIDeR***:

- ADAPT (Application Benefit Delivery Automation Project)
- APECS/iAPECS (Automated Program for the Enforcement of Child Support)
- ASAPS (Adult Services and Adult Protective Services)
- COOL
- DMV (Department of Motor Vehicles)
- eDRS
- FUEL/CRISIS
- MEDPEND
- OASIS (Online Automated Services Information System)
- SDX (State Data Exchange)
- SOLQ-I (SSA State Online Query)
- VACIS (Virginia Client Information System)
- VaCMS (Virginia Case Management System)
- VaMMIS (Virginia Medicaid Management Information System)
- VEC (Virginia Employment Commission)
- Work Number (3rd Party Employment information provided by TALX Corporation)

Notes:

- ***Confidential*** information in a legacy system will be ***confidential*** in SPIDeR.
- ***SPIDeR*** "times out" automatically after 30 minutes of inactivity.
- Each time a user's LDAP password changes, the ***SPIDeR*** password changes.

- System searches must have ***VALID*** business reasons.

- All ***SPIDeR*** transactions are documented in an audit log, which is subject to review.

VaCMS (Virginia Case Management System) automates the child care and the medical assistance program for the Division of Child Care & Early Childhood Development in VDSS.

EPPIC (Electronic Payment Processing and Information Control) system is used for the processing and maintenance of debit cards for clients (including the creation, delivery, and replacement of the physical debit card to the client).

ASAPS (Adult Services and Adult Protective Services) automation provides increased protection for seniors by establishing reporting requirements for Mandated Reporters as outlined by the APS Act passed by the Virginia General Assembly in 2004.

Related Reference:

IRS Publication 1075 (.pdf) - Tax Information Security Guidelines For Federal, State and Local Agencies.

4.11.1 ISRM Safeguards Program

The ISRM Safeguards program was implemented in June 2011 to ensure that VDSS is in compliance with the IRS, SSA, COV, and VDSS minimum protection standards for ***sensitive*** data. The safeguard review is an onsite evaluation of each Local Office, Regional Office, the Home Office, DCSE District Office, and the VITA Data Centers. The following key elements are the core of the Safeguard review:

a. Employee awareness of information security standards;

b. Record keeping;

c. Secure storage;

d. Limited access;

e. Information disposal; and

f. Actual computer systems security.

Related References:

IRS Publication 1075 (.pdf) - Tax Information Security Guidelines For Federal, State and Local Agencies.

New Approach to Federal Safeguards - Broadcast 7343 (.pdf)

See Safeguards

Social Security Program Rules

4.11.2 Data Storage Media Protection

Data storage media protection identifies the steps required for the appropriate handling of stored data to protect VDSS data from compromise. Logical and physical protection is required for all data storage media containing ***sensitive*** data, commensurate with ***sensitivity*** and ***risk***.

Storing any data classified as ***sensitive*** on any mobile device, including laptops and any non-network drive, but excluding backup media, is prohibited unless the data is encrypted and there is a written exception approved by the Commissioner or designee identifying the business case, risks, mitigating logical and physical controls, and any residual risk.

A vendor who stores ***sensitive*** information (as defined by VDSS) on their system must keep that data ***confidential,*** and destroy information after it is no longer necessary. Vendors should sign a ***Non-Disclosure Agreement*** to ensure that this is part of the contract.

Related Reference:

VDSS Nondisclosure Agreement (.pdf)

4.11.3 Encryption

To protect the ***confidentiality and integrity*** of ***sensitive*** information (e.g., ***PII***, and/or ***FTI***) stored in electronic form, it is necessary to encrypt that information "at rest" and in transit.

Data "at rest" is any ***sensitive information*** in files, databases, scanned documents, electronic faxes, etc., that is being stored electronically on devices like file servers, database servers, laptops, thumb drives, desktop hard drives, or portable hard drives. Encrypting data "at rest" protects the ***confidentiality*** of the data and prevents unauthorized use and viewing. On portable devices, encryption of data renders it useless if that device were stolen. VDSS users must not assume that data stored on a VITA or VDSS file server is encrypted. VDSS recommends using Microsoft Encrypting File System or WinZip with encryption and password to encrypt ***sensitive*** information that will be stored or transmitted over the Internet.

> *Note: VDSS allows the use of encrypted USB drives as long as the worker's supervisor has the password to the device. This process is required to ensure VDSS can access the data if the worker leaves. This exception to COV policy has been signed by the VDSS Commissioner.*

Sensitive data must be encrypted when in transit across networks to protect against eavesdropping of network traffic by unauthorized users. The types of transmission may include client-to-server, server-to-server, and any other data transfer between core systems and third party systems. All communications to and from state and local social service workers are transmitted through the Commonwealth's ***unencrypted*** enterprise network along with communications to and from many other state agencies.

Consider the following recommendations for the secure transit of VDSS/LDSS ***sensitive*** data:

a. If the device is reachable via a web interface, all web traffic must be transmitted using only strong security protocols such as Transport Layer Security (TLS);

b. Non-web transmission of ***sensitive*** data should be encrypted via application level encryption and connections between separate database and application servers must be encrypted to FIPS compliant cryptographic algorithms;

c. If application level security is not available or not FIPS compliant, implement network level encryption such as IPSec or SSH tunneling; and

d. ***Sensitive*** data transmitted over email must be secured using cryptographically strong email encryption tools such as PGP or S/MIME (see email paragraph below). Prior to sending the ***sensitive*** email/data, the user should encrypt the data using approved data "at rest" tools and attach the encrypted file to the email.

Examples of insecure network protocols and their secure alternatives include:

	Instead of…	**Use…**
Web Access	HTTP	HTTPS
File transfer	FTP, RCP	FTPS, SFTP, SCP, WebDAV over HTTPS
Remote shell	telnet	SSH2 terminal
Remote desktop	VNC	Radmin, RDP
Wireless	WEP, WPA, open access point	WPA2, SSID hiding, MAC ID filtering

Email is not considered secure and must not be used to transmit ***sensitive*** data unless additional email encryption tools are installed and used as previously described in d) above. VITA provides an encrypted email capability service for an additional fee to state agencies. A completed VITA Email Mailbox and Account Request Form is required for encryption email access requests. Completed and approved forms must be sent to security@dss.virginia.gov with a ***descriptive subject line*** such as "Encrypted Email Access Request – First Name Last Name."

Additional instruction/comments:

Does the user need the ability to send/receive encrypted e-mail? ☒ Yes ☐ No
Note: ISO Approval is required for encrypted e-mail requests

Related References:

Encryption Procedures Using Microsoft Word 2010 (.docx)

COV Email Mailbox and Account Request Form (.doc)

4.11.4 Data Sharing

Data held by, or provided to, VDSS must be properly managed and protected. To this end, data which VDSS shares with other organizations or receives to administer benefits and services must be controlled in a manner which meets security requirements.

Data sharing arrangements, either by Memorandum of Understanding (MOU), Memorandum of Agreement (MOA), contract, use agreement, or any such mechanism, must be approved by the VDSS CISO prior to any data movement or receipt. This includes data shared with other state and local agencies, their contractors, sub recipients, and the like. Similarly, the process by which the data will be transported, stored, and destroyed, as appropriate, must also be approved by the VDSS CISO.

Any data sharing requests outside of the above framework may need to follow FOIA procedures.

FTI cannot be shared.

Data must only be shared for purposes consistent with federal or state regulations.

4.11.5 Media Sanitization

If the PC is going to be used by another person coming into the same position, it is not necessary to wipe the hard drive.

Anytime VITA/NG removes a PC from the agency, they are required to wipe the hard drive of all information. To request a PC hard drive be wiped, submit a ticket to the VITA Help Desk.

If the PC or device to be sanitized contains ***FTI***, the sanitation process must conform to the requirement in the IRS Pub 1075.

> *Note: This standard applies to all electronic media that has memory such as the hard drives of personal computers, servers, mainframes, Personal Digital Assistants (PDAs), routers, firewalls, switches, tapes, diskettes, CDs, DVDs, cell phones, printers, and Universal Serial Bus (USB) data storage devices.*

Related References:

IRS Publication 1075 (.pdf) - Tax Information Security Guidelines For Federal, State and Local Agencies.

Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media (.pdf)

Removing Data

4.11.6 Record Retention

Employee security access records should be retained for three years or until audited whichever comes first.

Federal data should be retained for ten years. ***FTI*** should be destroyed after use or according to the agency record retention schedule. All other ***sensitive*** information including internal inspection records must be retained for three years or until audited or until no longer administratively useful.

Audit records must be retained for seven years to provide support for after-the-fact investigations of security incidents and to meet regulatory and agency information retention requirements.

4.11.6. a. Child Care and Development

Training and education documents including, but not limited to, curriculum, publications made available to child care providers, training materials such as handouts, videos, and activity books, surveys and results should be retained until updated or superseded then destroyed.

4.11.6. b. Division of Child Support Enforcement (DCSE)

For Closed Case Record: Obligated Legal Parent with Children Not Emancipated, the scheduled retention period is 10 years after closed and the confidential destruction method is indicated.

For Closed Case Record: Obligated Paid in Full with Children Emancipated, Obligated Cases Where Support Cannot Be Collected and Unobligated Cases, the scheduled retention period is three years after closed and the confidential destruction method is indicated.

4.11.6. c. Division of Licensing Programs

Licensed program provider files are to be retained five years after the facility or program closes.

Unlicensed program provider files are to be retained five years after the facility or program closes or completion of investigation into alleged unlicensed provider.

Voluntarily registered family day home provider files are to be retained five years after the facility closes.

4.11.6. d. Family Services

Adoption records are to be microfilmed and retained permanently.

Approved and denied applications from individuals providing care for a relative requiring assistance with

two or more activities of daily living (ADL) are to be retained for five years after distribution of funds or until audit, whichever is longer.

Court ordered requests for out-of-state child custody and visitation reports, also referred to as home studies, are to be retained for six months from the date of the Interstate Compact for the Placement of Children (ICPC) transmittal.

4.11.6. e. Office of Background Investigations

Central registry and release of information forms with matches to determine if an individual has a founded case of child abuse or neglect should be retained for 100 years after date of birth of individual. Criminal background investigations conducted on individuals seeking to provide services or care in Child Placing Agencies (CPA) or Children's Residential Facilities (CRF) should be retained for 100 years after date of birth of individual.

Related References:

IRS Publication 1075 (.pdf) - Tax Information Security Guidelines for Federal, State and Local Agencies.

Library of Virginia, Records Retention and Disposition Schedule – DCSE (.pdf)

Library of Virginia, Records Retention and Disposition Schedule – Department of Social Services – All Divisions (.pdf)

4.12 Facilities Security

Facilities security safeguards require planning and application of facilities' security practices to provide a first line of defense for information systems against damage, theft, *unauthorized* disclosure of data, loss of control over system ***integrity***, and interruption to computer services. For example, access to the VDSS computer facility is restricted to those individuals listed on the VDSS Computer Room Access List. Any individual not appearing on the list must be logged in and escorted by a VITA/NG employee. Furthermore, Sonitrol swipe cards protect the VDSS computer facility against physical access by *unauthorized* personnel. Physical access to essential computer hardware, wiring, displays, and networks is only provided to those individuals who need it to do their jobs. Facilities Security must conform to the requirements as stated in Section 9.3.11 Physical and Environmental Protection in the IRS Pub 1075. *Security Tip: Protecting **FTI** is everyone's responsibility. To prevent unauthorized access to **confidential FTI** data, verify the identity of all visitors/unauthorized individuals and have an authorized employee escort them while in a restricted area of the building.*

Related References:

IRS Publication 1075 (.pdf) - Tax Information Security Guidelines for Federal, State and Local Agencies.

Physical Security for Employees, Visitors and Property at Home Office – January 2006

4.13 Personnel Security

Personnel security controls reduce ***risk*** to VDSS systems and data by specifying access determination and control requirements that restrict access to these systems and data to those individuals who require such access as part of their job duties. Personnel security also includes Information Security Awareness Training program requirements to provide all information system users with appropriate understanding regarding the ***VDSS Information Security Policy and Program Guide*** and the ***VDSS Information Resource Acceptable Use Policy*** requirements for VDSS systems and data.

4.13.1 Logical Access Determination and Control

Personnel security refers to those practices, technologies and/or services used to ensure that personnel security safeguards are applied. Personnel security safeguards take into account: 1) granting or withdrawing physical and system access privileges upon hiring an employee, updating access, transferring an employee to another VDSS entity or state agency, terminating an employee, or when an employee resigns or changes job duties within a VDSS entity; 2) system access will be granted via a formal and auditable process; 3) initial security training will be conducted within 30 days of a new hire; 4) ***Non-Disclosure Agreements*** will be signed by all individuals who need access to ***sensitive*** information, prior to granting access to that information; and 5) background checks of personnel may be required consistent with VDSS entity policy and depending on the ***sensitivity*** of information accessible to that position.

The Security Access Management System (SAMS) provides a platform for the ISRM Office to grant, update and delete access as well as validate access granted to VDSS systems users and addresses the Auditor of Public Accounts (APA) Audit Report recommendations and findings delivered in December 2005.

LDAP is the system of record for VDSS which keeps a record of employee profiles and the systems to which they have access. LDAP account IDs must be unique. The LDAP IDs of former employees (full-time, P14, contractor, etc.) cannot be reused. Since SAMS matches the employee profile and the systems access privileges to the HR and VDSS systems and provides exception reports to the ISRM Office, any new system that needs to be brought in to the match process needs modifications to the LDAP administration tool as well.

The principle of ***Least Privilege*** must be followed for all employees who access VDSS systems.

A basic principle in information security, ***Least Privilege***, holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions.

Related Reference:

Approval Process Flow for VDSS Security Forms – Section 4.8.1.2 Account Management

4.13.2 New Employees

State/Local Security Officers are responsible for ensuring that new employees:

- Are provided a copy and requested to read the ***VDSS Information Security Policy and Program Guide***;
- Sign the ***VDSS Information Security – Policy Acknowledgement*** form; and
- Understand general security and Internet policies, practices and procedures.

State/Local Security Officers are responsible to:

- Provide system access required to perform their job based on ***BUSINESS NEED***;
- Add new employees to the ***Security Access Management System (SAMS)*** which will generate email for an Exchange Account to be built by Virginia Information Technologies Agency/Northrop Grumman (VITA/NG). (Some Local and/or share-support agencies do not use Exchange email.)
- Create and maintain a security folder for each employee with copies of approved system access request forms;
- Assist new employees with submitting entitlement information to the VCCC; and
- Assist new employees with access to the Knowledge Center. All new employees are required to complete ***VDSS Initial Information Security Awareness Training within 30 days of hire or transfer***.

4.13.3 Terminating or Transferring Employees

For terminations, supervisors are responsible for ensuring the Employee Separation & Transfer Checklist is completed and forwarded to their State/Local Security Officer for access removal immediately upon employee separation. The State Security Officer will save the document and email the completed form to: security@dss.virginia.gov, finance@dss.virginia.gov, general.services@dss.virginia.gov, and human.resources@dss.virginia.gov.

The COV domain and email accounts are terminated when the State/Local Security Officer terminates the employee's access in SAMS.

The following employment changes require that accounts for the old location be deleted ***first*** and then new accounts are added at the new location:

- Between LDSS locations

- VDSS position to LDSS position (or vice versa)
- DSS Contractor position to LDSS or VDSS position (or vice versa)

When processing the employee at the new location -- If the worker's email at the old agency was jane.doe@dss.virginia.gov, add her in SAMS (using her middle initial) as jane.a.doe@dss.virginia.gov.

Systems access (e.g., COV Domain/email) can be transferred *only* for employees moving from one VDSS State position to another VDSS state position. For example, if a DCSE state employee is moving to another DCSE state position, this process would be handled as a transfer. A Transfer Checklist must be submitted to Central Security (security@dss.virginia.gov) by the State Security Officer for the position the employee is leaving. The supervisor for the new position will need to complete and submit new access request forms (to include the SAMS Access Request Form and ***VDSS Information Security – Policy Acknowledgement*** form) for all access the Transfer employee requires for the new position.

*Note: System access **cannot** be transferred between LDSS locations.*

If a State/Local Security Officer is separating, the ***Director*** needs to submit a State/Local Security Officer Change Request Form.

Related Reference:

State/Local Security Officer Change Request Form (.docx)

Local Agency Employee Separation Checklist (.docx)

State Employee Separation & Transfer Checklist (.docx)

4.13.4 Seasonal Employees

Seasonal employees must have an LDAP account. Seasonal employees can be contractors. Only the Central Security Office processes contractors.

The Security Officer should suspend the seasonal worker's account any time they will be gone for more than 30 work days.

Seasonal workers with 90 to 179 days between work dates require an email to reset the account; the email must come from the person(s) who approved the original access request.

Seasonal workers with 180 days or more between work dates should be terminated. They must submit new request forms for access if/when rehired.

4.14 Contractors

The ***Third-Party Non-Disclosure Agreement*** will be used when a contractor will be given access to ***sensitive*** information systems and/or data for which there is a ***risk*** associated with data disclosure. The contractor shall take all precautions and measures necessary to ensure the ***integrity***, ***non-disclosure***, ***confidentiality*** and ***protection*** of all data and information obtained from VDSS including, but not limited to, all original reporting forms and data in any other form.

Contractors, who, for example, are asked to enter data into VDSS systems, including the Virginia Case Management System (VaCMS), are specifically required to:

1. Adhere to the current ***VDSS Information Resource Acceptable Use Policy;***

2. Adhere to the current *COV Information Security Standard*; and

3. Complete documents including the ***Non-Disclosure Agreement***, and ***Agency Request for Token (Reassignment)*** and any other system access forms as necessary.

Furthermore, the contractor's agency is responsible for the following system security requirements:

1. Obtain a criminal background check for all personnel who will be issued a Userid to access VDSS systems;

2. Submit Access Request Forms to the proper VDSS State/Local Security Officers in the prescribed format and means;

3. Ensure all individuals accessing VDSS information complete and attest to the completion of the required training prior to requesting access (i.e., complete the ***Initial Information Security Awareness Training***, read the ***VDSS Information Resource Acceptable Use Policy,*** and read and sign the ***VDSS Information Security – Policy Acknowledgement*** form and the ***Non-Disclosure Agreement***;

4. On the last day of employment/contract or the last day access is required, pertinent VDSS State/Local Security Officers must be notified on the provided access form of termination of employment/access and return/mail the Dual Factor Token to VDSS Information Security and Risk Management Office, 801 East Main Street, 7th Floor, Richmond, Virginia 23219;

5. Pay to replace any Dual Factor Tokens that are damaged or lost by employees/contractors. Cost will be based on replacement cost at time of purchase; and

6. Prohibit the downloading or copying of any information contained in VDSS systems to any other computer system or computer application.

Employees/contractors who require access to the COV's network and VDSS systems must abide by the following conditions:

1. Read and comply with the ***VDSS Information Security Policy and Program Guide*** requirements provided by VDSS State/Local Security Officers including updates and revisions;

2. Read and sign a ***Non-Disclosure Agreement*** before being granted access to VDSS systems;

3. Read and sign the ***VDSS Information Security – Policy Acknowledgement*** form to indicate the reading and acknowledgement of VDSS security policies and procedures;

4. Complete the ***VDSS Information Security Awareness Training annually*** via the COV Knowledge Center;

5. Not use COV-provided network access credentials from any location other than the business address for the contractor and affiliates listed, especially not from home or any public access systems such as a public library, school, or commercial hot spot;

6. Protect and properly use the Dual Factor Token provided to access VDSS system(s). Use of the token is restricted to the individual to whom the token was issued;

7. Report a lost/missing Dual Factor Token within 24 hours of discovery to the VDSS CISO (security@dss.virginia.gov) or (804) 726-7153; and

8. Take reasonable and prudent steps to protect the security of information systems and data to which they have access.

   Notes:

   - *Contractor access to VDSS information systems* ***absolutely*** *must follow* ***least privilege.***

   - *The VDSS Sponsor is required to maintain contractor access information, including Access Request Forms.*

   - ***All*** requests for contract worker access must be submitted to the Central Security Office (CSO); Only the CSO may grant access to contract workers.

   - Contractors **MUST** only be entered into SAMS by the CSO.

4.14.1 Equipment and Software Ownership

Contractors and/or affiliates must:

1. Obtain approval from the VDSS CISO before connecting any equipment to the COV network.

2. Own all equipment (computers, printers, network and storage devices) that are connected to the COV's network and used to access VDSS systems;

3. Purchase and install a CISCO VPN software solution;

4. Purchase and install an Anti-Virus product and provide proof of current Anti-Virus product usage upon request;

5. Own all software including Internet Explorer used to access VDSS systems; and

6. Up-to-date software patches must be applied.

4.14.2 Reporting

The *contracting agency* will report annually, on the contract renewal date or upon change to any of the following items, to the Central Security Office:

1. Complete list of all equipment to include manufacturer, model, and serial number;

2. Proof of Purchase or certification of Anti-Virus program for each computer in Item 1 above;

3. Proof of Purchase for all software related to the VDSS project loaded on the computers in Item 1 above;

4. List of current employees working under the authority of this contract and the address(es) from which staff will be working and accessing the COV network and the VDSS application(s);

5. Copy of a written contract that binds the listed affiliate agencies to the requirements of this contract; and

6. Updated software patches must be certified.

4.14.3 Contractor Monitoring

The VDSS Sponsor is required to maintain accurate records of contractors, including their ***VDSS Information Security – Policy Acknowledgement*** form. The ISRM Office maintains contractor information on SPARK.

4.15 Information Security Awareness Training Program

The ***Information Security Awareness Training Program*** focuses on identifying ***risks***, threats, and vulnerabilities of VDSS information systems and how to fix them.

Topics covered in security awareness training include:

- The nature of ***sensitive*** material and physical assets encountered during routine business;

- Employee and contractor responsibilities in handling ***sensitive*** information, including review of employee Non-Disclosure agreements;

- Requirements for proper handling of ***sensitive*** material, including marking, transmission, storage and destruction;

- Proper methods for protecting ***sensitive*** information on computer systems, including password policy and use of two-factor authentication;

- Other computer security concerns including malware, phishing, social engineering, etc.

- Workplace security including building access, wearing of security badges, reporting of incidents, forbidden articles, etc.; and

- Consequences of failure to protect information, including potential loss of employment, economic consequences to VDSS and the COV, damage to individuals whose private records are divulged, and possible civil and criminal penalties.

The VDSS ISRM Office has developed several methods of accomplishing its ***Information Security Awareness Training Program*** objectives:

- ***Initial Information Security Awareness Training –*** Complete required online course in the Knowledge Center within the first 30 days of employment;

- ***Annual Information Security Awareness Training -*** Present to all employees annually using the Knowledge Center;

- ***Information Security Program*** - Supply each employee with a copy of the ***VDSS Information Security Policy and Program Guide***; and

- **Emails and Broadcasts** - Inform individuals of information security concerns, issues and warnings using various electronic communication formats such as direct emails and SPARK Broadcast messages.

4.16 Information Resource Acceptable Use Policy

VDSS provides computers and computer accounts to its staff to assist them in the performance of their jobs. The computer systems and networks belong to VDSS, and the user may use the system for authorized purposes only. The ***VDSS Information Resource Acceptable Use Policy*** is an integral part of the framework of the ***VDSS Information Security Program***. New employees and contractors of VDSS are required to sign the ***VDSS Information Security – Policy Acknowledgement*** form before access to information systems and data is granted. Acceptable use of the Internet consists of activities necessary to support the purpose, goals, and mission of VDSS divisions/directorates/offices/districts/regions and LDSS and each user's authorized job functions as expressed in either the Employee Work Profile (EWP) or the Contractor Statement of Work (SOW).

Personal use of the Internet is permitted during:

- Established lunch periods – Usage must be less than 15 minutes in any continuous hour;
- Break periods – Usage must be less than 5 minutes; and
- Before and after established work schedule – Less than 15 minutes in any continuous hour.

Use of personally-owned equipment such as scanners, Universal Serial Bus (USB) thumb drives, smart phones and computers to store and/or process information *that has been determined to be* ***sensitive*** during a RA or BIA is strictly prohibited and not allowed by COV Standards.

Compliance with the ***VDSS Information Resource Acceptable Use Policy*** is measured by regular audits.

Related Reference:

VDSS Information Resource Acceptable Use Policy (.pdf)

4.17 Asset Management

Asset management, maintained by VDSS DIS, concerns protection of the components that comprise VDSS systems by managing them in a planned, organized and secure fashion. Asset management includes asset control, software license management, configuration management, and change control.

4.17.1 Asset Control

Asset Control must be commensurate with ***sensitivity*** and ***risk***, and policies and procedures must be applied accordingly. IT personnel are encouraged to maintain their own records, especially those components that are associated with the BIAs and RA processes. VDSS should ensure asset management is a component of the current asset management program. Access to asset inventory records should be restricted to a need-to-know basis. IT employees may be of assistance when an asset inventory is conducted since some components are difficult to identify if included within a larger system.

The VITA/NG partnership maintains the inventory of hardware for all of VDSS locations. DIS is then billed for VITA/NG hardware deployed at VDSS locations throughout the state. It is not mandated by VITA/NG or DIS that VDSS sites maintain an inventory listing. Still, all of VDSS locations and offices have certain responsibilities to promote the ability for inventory to be properly managed.

There are several processes DIS uses to identify possible inventory errors. DIS routinely “spot checks” for accuracy as well as investigates discrepancies. These processes help detect idle equipment, old equipment, assets assigned to an incorrect location or function, refresh activities as well as other inventory-related activities. Assets will be researched for business necessity and proper use. DIS will utilize and maintain a POC list for all VDSS locations and contact them as necessary to address any inventory concerns or questions.

Related References:

Controlled Asset Inventory of Office Equipment and Furnishings (.doc)

IT Asset Management Policy and Procedures (.pdf)

Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (.pdf)

Surplus Computer Equipment Removal Request (.doc)

Telecommunications Policy and Procedures (.pdf)

4.17.2 Software License Management

Maintenance of proper security software requires that all VDSS divisions/directorates/offices/districts/regions and LDSS take necessary steps to ensure proper software and documentation is maintained for all COV systems. Only VDSS-approved software may be installed on VDSS information systems. Non-VDSS provided software may be installed on VDSS computers if approved by the NG Service Level Director (SLD) and the VDSS CISO.

- **IMPORTANT!** LDSSs are responsible to maintain an accurate accounting of all locally purchased software and ensure compliance with all aspects of the vendor licensing agreement(s).

- Before installing any non-standard software on a state computer, complete the software request form and email it to security@dss.virginia.gov. Once approved, contact the VITA Customer Care Center (VCCC) and request that a technician install the software.

NOTE: State software cannot be provided for locally-owned servers, desktop or laptop computers.

Any VDSS/LDSS user has approval per the VDSS CISO to operate the "Go to Meeting" and WebEx software on any VDSS/LDSS computer. Individuals may submit VCCC tickets for this software when they are unable to attend a meeting. It is not always possible to plan attendance at these requested meetings being hosted by numerous federal, state, and industry sources in advance.

Related References:

IT Asset Management Policy and Procedures (.pdf)

Non-VDSS Provided Software Request (.doc)

4.17.3 Configuration Management and Control

Configuration Management and Change Control practices must be in place so that changes to the IT environment do not compromise VDSS security controls. Configuration Management is required per the ***VDSS Software Development Lifecycle Manual (SDLM)*** via the Project Management Plan. The VDSS Information Technology Change Management Process describes the process and provides a definition of the management controls required to better manage overall ***risks*** and changes to the IT production environments. Depending on the type of change, the process begins with either a Service Request for major projects, or a Change Request for lower ***risk*** or administrative changes.

Related References:

Business Process Re-Engineering

DSS IT Change Management Process (.pdf)

Database Change Request (.doc)

Service Request

Software Development Lifecycle Methodology (SDLM)

Software Development Lifecycle Manual Reference Manual (.docx)

Software Quality Assurance (SQA)

4.18 Removable Media

The use of personal thumb drives (USBs) is expressively prohibited. The use of a home router/modem is permitted as long as the connection is through the COV VPN.

5. Incident Reporting

1. Any suspected or inappropriate access or suspected improper updating of information must be reported to the VDSS CISO (security@dss.virginia.gov) immediately;

2. The report shall include:

   a. Name of person making the report;

   b. Contact information to include telephone number, email and mailing address; and

   c. Brief description of the ***Information Security Incident***.

3. Information requested by the VDSS CISO relating to ***Information Security Incidents*** or employee access issues must be provided within 48 hours of request in a *written* form.

Related References:

VDSS Nondisclosure Agreement (.pdf)

Initial Incident Reporting Form (.docx)

6. Compliance

All VDSS divisions/directorates/offices/districts/regions and LDSS are responsible for ensuring compliance with information security policies and standards. VDSS measures compliance with information security policies and standards through processes that include, but are not limited to:

- Inspections, reviews, and evaluations;
- Monitoring;
- Audits; and
- Confiscation and removal of information systems and data.

6.1 Proactive Monitoring

In support of the Commonwealth's efforts to strengthen the public trust by more effectively monitoring how resources are used, NG invested in ***McAfee Secure Web Gateway*** and ***Blue Coat Security Platform - Reporter***. With these applications and proper authorization, VDSS can monitor and create reports on Internet usage by state and local employees. Monitoring of VDSS information systems and data may include, but is not limited to: network traffic; application and data access; keystrokes and user commands; email and Internet usage; and message and data content.

Monitoring is used to improve information security, to assess appropriate use of VDSS information resources, and to protect those resources from attack. Use of VDSS information resources constitutes permission to monitor that use. There should be no expectation of ***privacy*** when utilizing VDSS information resources. VDSS reserves the right to:

a. Review the data contained in or traversing VDSS information resources;

b. Review the activities on VDSS information resources;

c. Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the VDSS CISO; and

d. Scan VITA/VDSS devices to ensure software, patching, and security controls are up-to-date.

SPIDeR:

All searches performed in SPIDeR are logged. The information logged includes, but is not limited to, the worker's LDAP ID, the date and time of the search, and the data (client's name, Social Security Number [SSN], case number, etc.) on which the search was performed. This allows the VDSS ISRM Office to see what searches a worker has performed. The VDSS ISRM Office can determine which workers and what information employees have searched about a specific client or case.

Each month, one or more local agencies and VDSS offices are randomly selected. Then, one or more workers (who used SPIDeR) at each of these offices are randomly select for review. The searches performed by these workers are extracted from the SPIDeR Audit Log and sent to LDSS management and State/Local Security Officers. The appropriateness of the searches is then determined by that LDSS management and State/Local Security Officers.

Inappropriate searches may result in termination of employment, being charged with a federal felony offense, and up to a $5,000 fine.

Related Reference:

New Proactive Monitoring Program – ISRM Broadcast 7639 (.pdf)

6.2 Requesting and Authorizing Monitoring

Requests for reports cannot be made arbitrarily; they must be for a ***justifiable*** reason.

Requests for monitoring are made by the Director or Division Head and sent to the VDSS CISO. The VDSS CISO has the responsibility to authorize monitoring or scanning activities for network traffic, application and data access, keystrokes and user commands, and email and Internet usage, and message and data content for VDSS information systems and data. The VDSS CISO and the VDSS ISO shall notify each other when appropriate. All communications to the LDSS or Division will include distribution to the LDSS or Division Director.

Related References:

Audit Log Internet/EAL/SPIDeR Request (.docx)

Incident Management and Internet/EAL/SPIDeR Request Flowchart (.xlsx)

Initial Incident Reporting Form (.docx)

6.3 Security Audits

As required by COV in the *Information security Audit Standard,* VDSS is to conduct Information security audits of systems and government databases which contain ***sensitive*** information. For security purposes, the ISRM Office must also ensure that federally-sourced data is appropriately secured and controlled. In this section, ***sensitive*** information also includes data which is federally-sourced.

The protection of VDSS-held data is also, in some cases, prescribed by law. Client information gathered and used for purposes of administering programs and providing services, in many situations, can only be used for those purposes and the information cannot be distributed or shared for any other purpose either inside or outside of VDSS and LDSS.

If ***sensitive*** systems contain federal data, such as that received from the IRS and the SSA, there are additional protections which must be in place and functioning to meet federal requirements. One example of the protections around federally-sourced data prescribes that all worker views of ***FTI*** via VDSS systems must be logged and the logs retained for six years.

6.4 Proactive Monitoring Program and Enterprise Audit Log (EAL) Tool

The ***Proactive Monitoring Program*** and the ***Enterprise Audit Log (EAL) Tool*** identify inappropriate transactions conducted by individuals using VDSS information systems. ISRM personnel can use these tools to determine who attempted what action, in which system, on what data, and when that operation was attempted. This information is required to:

- Preserve VDSS's rights and remedies in the event of data being compromised by accidental or intentional disclosure or by alteration;
- Comply with audit logging requirements for the IRS (as identified in IRS publication 1075);
- Comply with audit logging requirements for the SSA (as identified in Information System Security Guidelines for Federal, State and Local Agencies Receiving Electronic Information from the Social Security Administration);
- Comply with COV audit logging requirements (as identified in ITRM Standard SEC501); and
- Comply with audit log requirements for any other non-VDSS systems such as DMV, VEC, DMAS, and/or others that are accessed electronically by “VDSS systems.”

7. Process for Requesting Exception to the VDSS Information Security Program

If the Commissioner determines that compliance with the provisions of the *COV Information Security Policy* or related standards would result in a significant adverse impact to VDSS, the Commissioner may request approval to deviate from that security policy requirement by submitting an exception request to the COV CISO.

If division/directorate/office/district/regions and LDSS management determines that compliance with the provisions of the VDSS information security policies, standards, and guidelines or related standards would result in significant adverse impact to their division/directorate/office/district/regions and LDSS, the director or senior manager may request approval to deviate from that information security policy requirement by submitting an exception request to the VDSS CISO.

Each request shall be in writing and include a statement detailing the reasons for the exception and compensating controls. Requests for exception shall be evaluated and decided upon by the VDSS CISO or the VDSS ISO as appropriate and the requesting party informed of the action taken. Denied exception requests may be appealed to the COV CISO or the VDSS CISO as appropriate.

Related References:

VDSS Information Security Exceptions and Exemptions Policy

VDSS Information Security Policy and Standard Exception Request Form

VDSS Standard Risk Exception and Acceptance Request Form

8. Related Information Security Policies, Procedures, Guides and Manuals

ISRM SPARK website

State/Local Security Officers Procedures Manual (.pdf)

Security Access Management System (SAMS) Manual (.pdf)

VDSS Business Impact Analysis Policy

VDSS Configuration Management Policy

VDSS Disaster Recovery Staffing Policy

VDSS Enterprise Background Check Policy

VDSS Information Resource Acceptable Use Policy (.pdf)

VDSS Emergency Response Damage Assessment Procedure

VDSS Information Security Assessment and Authorization Policy

VDSS Information Security Audit, Monitoring and Logging Policy

VDSS Information Security Awareness and Training Policy

VDSS Information Security Exceptions and Exemptions Policy

VDSS Information Security Glossary

VDSS Information Security Incident Reporting Procedure

VDSS Information Security Incident Response Plan

VDSS Information Security Incident Response Policy

VDSS Information Security Incident Response Procedure

VDSS Information Security Policy and Standard Exception Request Form

VDSS Information Security - Policy Acknowledgement (.pdf)

VDSS Information Security Roles and Responsibilities Policy

VDSS Information System and Communications Encryption Policy

VDSS Information System and Communications Protection Policy

VDSS Information System and Data Classification Policy

VDSS Information System and Information Integrity Policy

VDSS Information System and Services Acquisition Policy

VDSS Information System Contingency Planning Policy

VDSS Information System Identification and Authentication Policy

VDSS Information System Maintenance Policy

VDSS Information System Security Planning Policy

VDSS Logical Access Controls Policy

VDSS Media Protection Policy

VDSS Mobile Device Access Controls Policy

VDSS Personnel Security Policy

VDSS Physical and Environmental Protection Policy

VDSS Remote and Wireless Access Controls Policy

VDSS Reportable Information Security Incident Guide

VDSS Risk Assessment Policy

VDSS Standard Risk Exception and Acceptance Request Form